INFORMATION TO USERS

This reproduction was made from a copy of a document sent to us for microfilming. While the most advanced technology has been used to photograph and reproduce this document, the quality of the reproduction is heavily dependent upon the quality of the material submitted.

The following explanation of techniques is provided to help clarify markings or notations which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to assure complete continuity.
2. When an image on the film is obliterated with a round black mark, it is an indication of either blurred copy because of movement during exposure, duplicate copy, or copyrighted materials that should not have been filmed. For blurred pages, a good image of the page can be found in the adjacent frame. If copyrighted materials were deleted, a target note will appear listing the pages in the adjacent frame.
3. When a map, drawing or chart, etc., is part of the material being photographed, a definite method of "sectioning" the material has been followed. It is customary to begin filming at the upper left hand corner of a large sheet and to continue from left to right in equal sections with small overlaps. If necessary, sectioning is continued again—beginning below the first row and continuing on until complete.
4. For illustrations that cannot be satisfactorily reproduced by xerographic means, photographic prints can be purchased at additional cost and inserted into your xerographic copy. These prints are available upon request from the Dissertations Customer Services Department.
5. Some pages in any document may have indistinct print. In all cases the best available copy has been filmed.

**University
Microfilms
International**

300 N. Zeeb Road
Ann Arbor, MI 48106

8518999

Narang, Kamal

**THE GROUP OF AUTOMORPHISMS OF NON-ASSOCIATIVE COMMUTATIVE
ALGEBRAS ASSOCIATED WITH $PSL(M, Q)$, M GREATER THAN OR EQUAL
TO 3**

The Ohio State University

Ph.D. 1985

**University
Microfilms
International** 300 N. Zeeb Road, Ann Arbor, MI 48106

THE GROUP OF AUTOMORPHISMS
OF NON-ASSOCIATIVE COMMUTATIVE ALGEBRAS
ASSOCIATED WITH $\text{PSL}(m,q)$, $m \geq 3$

DISSERTATION

Presented in Partial Fulfilment of the Requirements for
the Degree Doctor of Philosophy in the Graduate
School of The Ohio State University

By

Kamal Narang, B.Sc., M.Sc.

The Ohio State University

1985

Reading Committee:

Dr. K. Harada

Dr. S.K. Wong

Dr. R. Solomon

Approved by

Adviser
Department of Mathematics

ACKNOWLEDGMENTS

I wish to express my deep and sincere gratitude to my adviser, Professor K. Harada for the ample help, the kind treatment, the very patient guidance and the constant encouragement I received from him.

Professor S.K. Wong provided me with many useful hints and ideas. One of his observations is of extreme importance to my method of determining the automorphism group.

A computer program written for me by my friend and colleague Dr. Joseph D'Mello enabled me to determine the automorphism group in a particular case when I did not have any method to attack the problem in general.

Professor R. Solomon read the draft of this thesis and made numerous suggestions to improve the text.

I am grateful to all these people.

VITA

August 27, 1948 Born - Allahabad, India
1968 B.Sc., University of Allahabad,
Allahabad, India
1970 M.Sc.(Statistics), University
of Allahabad, Allahabad, India
1973 M.Sc.(Mathematics), Indian
Institute of Technology, Kanpur,
India
1973-1977 Graduate Student, Centre of
Advanced study in Mathematics,
University of Bombay, Bombay,
India
1978-1985 Graduate Teaching Associate,
Department of Mathematics,
The Ohio State University,
Columbus, Ohio

FIELDS OF STUDY

Major Field: Group Theory

Studies in Group Theory. Professor K. Harada

TABLE OF CONTENTS

	Page
ACKNOWLEDGEMENT	ii
VITA	iii
INTRODUCTION	1
 CHAPTER	
I. COMMUTATIVE ALGEBRAS ASSOCIATED WITH DOUBLY TRANSITIVE PERMUTATION GROUPS AND AUTOMORPHISM GROUPS OF THESE ALGEBRAS	12
1. Permutation Groups and commutative Algebras	12
2. Doubly Transitive Permutation Groups and Commutative Algebras	16
II. COMMUTATIVE ALGEBRAS ASSOCIATED WITH $PSL(m, q)$, $m \geq 3$	20
1. The Group $PSL(m, q)$	20
2. Action of $PSL(m, q)$ on $PG(m-1, q)$	21
3. The Algebra A	24
III. AUTOMORPHISM GROUP OF THE ALGEBRA A ASSOCIATED WITH $PSL(m, q)$, $m \geq 3$	25
1. The Algebra A	25
2. The Regular Representation of A	25
3. The Automorphism Group of A	27
IV. DETERMINATION OF THE AUTOMORPHISM GROUP OF A IN THE CASE $b = 0$	31
1. The Algebra A	31
2. The New Algebra B, its subset A^*	31
3. The Relation Obtained from the Minimal Polynomial	35
4. Calculation of the Automorphism Group of A	37

V. DETERMINATION OF THE AUTOMORPHISM GROUP OF A IN THE CASE $b = a + c$, $b \neq 0$, $c \neq 0$	47
1. The Algebra A	47
2. The Relation Obtained from the Minimal Polynomial	49
3. Calculation of the Automorphism Group of A	49
LIST OF REFERENCES	88

INTRODUCTION

Let V, W be vector spaces over a field F . A multilinear map θ of degree r from V to W is a map

$$\theta : V \times V \times \dots \times V \longrightarrow W$$

which is linear in each co-ordinate. θ is called symmetric if $\theta(v_1, v_2, \dots, v_r) = \theta(v_{\tau(1)}, v_{\tau(2)}, \dots, v_{\tau(r)})$ for all τ in Σ_r , the symmetric group of degree r . θ is called non-singular if $v \neq 0$ implies $\theta(v, v, \dots, v) \neq 0$.

If $W = V$, we call θ a multilinear map of degree r on V , and if $W = F$, we call θ a multilinear form of degree r on V .

For a multilinear map θ of degree r on V , the automorphism group of θ , denoted by $\text{Aut}(\theta)$, is the subgroup of $\text{GL}(V)$ defined by

$$\text{Aut}(\theta) = \left\{ \sigma \in \text{GL}(V) : \theta(v_1, v_2, \dots, v_r)^\sigma = \theta(v_1^\sigma, v_2^\sigma, \dots, v_r^\sigma) \forall v_i, 1 \leq i \leq r \right\}$$

If θ is a multilinear form of degree r on V , $\text{Aut}(\theta)$ is defined as

$$\text{Aut}(\theta) = \left\{ \sigma \in \text{GL}(V) : \theta(v_1, v_2, \dots, v_r) = \theta(v_1^\sigma, v_2^\sigma, \dots, v_r^\sigma) \forall v_i, 1 \leq i \leq r \right\}$$

An interesting and long-standing problem has been to determine conditions under which $\text{Aut}(\theta)$ is a finite group. The first result is due to Jordan [13], which states that if θ is a non-singular symmetric multilinear form of degree $r > 2$ on a vector space V over the field of complex numbers, then $\text{Aut}(\theta)$ is finite.

Schneider [17] extended Jordan's result to fields of characteristic zero or greater than r . But Schneider's proof contains an error (see Suzuki [19]). Some other related results are by Matsumura and Monsky [15] and Sah [16]. These use methods of algebraic geometry.

The latest results in this context are by H. Suzuki [19] and Y. Egawa and H. Suzuki [5]. Put together, the two results state that if θ is a non-singular multilinear map of degree $r \geq 2$ on a vector space V over an algebraically closed field, then $\text{Aut}(\theta)$ is finite. However, it is not an easy task to determine the non-singularity of a multilinear map θ . Also, there exist singular multilinear maps θ for which $\text{Aut}(\theta)$ is finite. For example, the bilinear map which gives the n -dimensional algebra described by Harada [9] is non-singular if and only if $\gcd(2p, n+1) = 1$, where $p = \text{ch}(F)$ if $\text{ch}(F) > 0$, and $p = 1$ if $\text{ch}(F) = 0$. However, $\text{Aut}(\theta) \cong \Sigma_{n+1}$, the symmetric group of degree $n+1$ if $\text{ch}(F) = 0$ or $\text{ch}(F) > n+1$. (See Harada [9])

Symmetric multilinear maps of degree 2 and degree 3, that is, symmetric bilinear and trilinear maps have been studied in this context by many mathematicians in the recent past. If θ is a symmetric bilinear map on V , we can define a binary product on V given by

$$vw = \theta(v, w), \quad v, w \in V$$

This provides V with a commutative algebra structure, which is invariant under $\text{Aut}(\theta)$. Conversely, any commutative algebra structure on V gives rise to a symmetric bilinear map. Hence the notion of a commutative algebra is equivalent to that of a symmetric bilinear map. Trilinear maps can also give an algebra structure under some conditions.

An interesting problem has been to construct algebras invariant under the action of certain specific groups, and the determination of the automorphism groups of these algebras. This becomes particularly interesting if the group can be recovered from $\text{Aut}(V)$, that is to say, if $\text{Aut}(V)$ is not "too far away" from the group. Usually it is not easy to determine the automorphism group of an algebra (see Suzuki [19]).

S. Norton constructed commutative algebras, known as "Norton Algebras". The automorphism groups of these algebras contain finite groups generated by 3-transpositions. His method is to take the permutation module

defined by the rank 3 action of a group on a conjugacy class of 3-transpositions and to define algebra structure on the non-trivial irreducible factors. Cameron, Goethals and Siedel [4] generalized Norton's method to show that the Norton Algebra can be defined for a large class of transitive groups. Smith [18] studied the problem of determining the automorphism group of a Norton algebra. His method is to construct a graph on a class of 3-transpositions by joining the commuting pairs, which he does for a triple cover of a 3-transposition group. The automorphism group of the smallest (12-dimensional) algebra is determined to be $3\Sigma_7$. But it seems very hard to tackle such questions in general.

The most important result in this context is the beautiful construction of the Monster Simple Group by Griess [8]. He exhibited the existence of a 196883-dimensional commutative (non-associative) algebra V invariant under the action of Monster Simple Group, and showed that a certain subgroup of $\text{Aut}(V)$ is isomorphic to the Monster Simple Group.

To show that $\text{Aut}(V)$ is finite, Griess has a rather involved argument, using deep results of finite group theory. In a recent paper, Tits [24] has simplified Griess' proof by showing that if a C -invariant bilinear

map θ on the Griess' algebra V satisfies a certain condition, then $\text{Aut}(\theta)$ is finite. Here C is the centralizer of an involution of the Monster Simple Group, and is an extension of the Conway's group .1 by an extra special group of order 2^{1+24} . (See also Tits [21], [22], [23])

Motivated by the work of Griess, Harada [9], [10] considered the automorphism group of a non-associative, commutative algebra obtained from the permutation action of a multiply transitive group. His work provides the backbone to this thesis, and is discussed in chapters I and II.

Allen [1] determined the automorphism group of the algebra given by Harada for a triply transitive group acting on a set of $n+1$ elements when the characteristic of the underlying field ($\neq 0$) is less than or equal to $n+1$.

Frohardt [7] has constructed a commutative algebra invariant under the action of J_3 , one of Janko's simple groups. He starts with an action of J_3 on an 85-dimensional vector space V over the field $F = \mathbb{Q}(\sqrt{-3}, \sqrt{-19})$ to obtain a J_3 -invariant symmetric trilinear form θ on V . He then uses θ to obtain a J_3 -invariant commutative algebra structure on $V \otimes V^*$, where V^* is the dual of V as a J_3 -module.

Wajima [25] considers "almost alternating" algebras. An algebra V over a field F with a basis $\{v_1, v_2, \dots, v_n\}$ is called almost alternating (to be written a.a. henceforth) if

$$v_i v_i = v_i, \quad 1 \leq i \leq n$$

$$v_i v_j = -v_j v_i, \quad 1 \leq i < j \leq n$$

Wajima showed that for an a.a. algebra V of dimension n , $\text{Aut}(V)$ is isomorphic to a subgroup of Σ_n , and is isomorphic to Σ_n if and only if there exists λ in F such that

$$v_i v_j = \lambda(v_i - v_j), \quad 1 \leq i \neq j \leq n$$

He further showed that any permutation group gives rise to a non-trivial a.a. algebra V . If G acts triply transitively on a set Ω of order n , then the algebra structure of V is uniquely determined, and $\text{Aut}(V) \cong \Sigma_n$. However if G is sharply triply transitive on Ω , then one can define an a.a. algebra V for which $\text{Aut}(V) \cong G$. He also studied a.a. algebras obtained from orthogonal groups.

Wajima [25] constructed a commutative algebra invariant under the action of Mathieu group M_{12} , by considering an absolutely irreducible representation of M_{12} of degree 45.

Using the idea of Tits [24], Kitazome [14] has recently obtained $\Omega^-(6,3)$, $\Omega(7,3)$ and the Fischer group F_{24} as the groups of automorphisms of corresponding commutative algebras of dimensions 42, 54 and 783 respectively.

Y. Egawa and H. Suzuki [6] studied Σ_{n+1} -invariant symmetric trilinear forms ($n \geq 2$) over the field of complex numbers, and determined the structure of the automorphism group of any Σ_{n+1} -invariant symmetric trilinear form if $n \neq 3$. Let V be an n -dimensional vector space over the field of complex numbers with basis $\{v_1, v_2, \dots, v_n\}$. Let $v_{n+1} = -v_1 - v_2 - \dots - v_n$. Then V is a natural irreducible Σ_{n+1} -module, with the standard action of Σ_{n+1} on the set $\{1, 2, \dots, n+1\}$, and so Σ_{n+1} can be regarded as a subgroup of $GL(V)$. Let θ_n be the Σ_{n+1} -invariant symmetric trilinear form on V defined by

$$\theta_n(v_i, v_i, v_i) = n(n-1), \quad 1 \leq i \leq n$$

$$\theta_n(v_i, v_i, v_j) = -(n-1), \quad 1 \leq i \neq j \leq n$$

$$\theta_n(v_i, v_j, v_k) = 2, \quad 1 \leq i \neq j \neq k \leq n$$

Egawa and Suzuki showed that if θ is any Σ_{n+1} -invariant symmetric trilinear form on V , then $\theta = \xi \theta_n$, where ξ is a non-zero complex number. Hence $\text{Aut}(\theta) \cong \text{Aut}(\theta_n)$. They further showed that if $n = 2$, or $n \geq 4$, then $\text{Aut}(\theta_n) \cong \langle \omega I \rangle \times \Sigma_{n+1}$, where I is the identity of $GL(V)$

and $\omega = \frac{-1 + \sqrt{-3}}{2}$ is a cube root of unity.

Our work concerns the projective special linear group $\text{PSL}(m, q)$. Let $G = \text{PSL}(m, q)$. Then G acts doubly transitively on the set $\Omega = \{1, 2, \dots, n+1\}$, where $n = \frac{q^m - q}{q-1}$. If $m \geq 3$, the global stabilizer $G_{i,j}^*$ of the set $\{i, j\} \subset \Omega$ has exactly two orbits on the set $\Omega \setminus \{i, j\}$, the shorter one having length $q-1$. Let us denote this orbit by $L(i', j')$. The G -invariant commutative non-associative algebra A over a field K with basis $\{x_1, x_2, \dots, x_n\}$ constructed by Harada [10] for any doubly transitive permutation group reduces in this case to the following structure:

$$(1) \begin{cases} x_i x_i = ax_i, & 1 \leq i \leq n+1 \\ x_i x_j = b(x_i + x_j) + c \sum_{k \in L(i', j')} x_k, & 1 \leq i < j \leq n+1 \\ \text{where } a, b, c \in K \text{ and satisfy the relation} \\ a + (n-1)b = (q-1)c. & x_{n+1} = -x_1 - x_2 - \dots - x_n. \end{cases}$$

The multiplication by x_1 gives a K -endomorphism of A . Harada [11] showed that the minimal polynomial $m(X)$ of the multiplication by x_1 , $1 \leq i \leq n+1$, is given by

$$m(X) = \begin{cases} (X-a)(X-b), & \text{if } c = 0 \\ (X-b+c)(X-b-(q-1)c), & \text{if } b(a+c-b) = 0, c \neq 0 \\ (X-a)(X-b+c)(X-b-(q-1)c), & \text{otherwise} \end{cases}$$

If $c = 0$, $\text{Aut}(A)$ was determined by Harada [9] and Allen [1].

We have determined the automorphism group of A in the second case, that is, if $b(a+c-b) = 0$, $c \neq 0$, under certain restrictions on the characteristic of the field K , and shown it to be the projective semi-linear group $P\Gamma L(m, q)$. Stated precisely, our result is:

Theorem : Let $G = \text{PSL}(m, q)$, $m \geq 3$. Let A be the algebra over the field K with basis $\{x_1, x_2, \dots, x_n\}$ and multiplication given by (1). Then $\text{Aut}(A) \cong P\Gamma L(m, q)$ if one of the following holds:

(i) $b = 0$, $c \neq 0$ and $n+1 \neq 0$ in K , $q-1 \neq 0$ in K and $q+1 \neq 0$ in K .

(ii) $b = a+c$, $b \neq 0$, $c \neq 0$ and the characteristic of K is zero or greater than $\frac{q^m-1}{q-1}$ and $n+1 \neq 0$ in K .

In chapter I we discuss Harada's results on commutative algebras associated with doubly transitive permutation groups and automorphism groups of these algebras.

In chapter II we study the doubly transitive action of $\text{PSL}(m, q)$ on a set of $n+1$ elements, $n = \frac{q^m-1}{q-1}$, the orbit structure of this action, and the algebra A given by this action.

In chapter III we develop the necessary tools for determining the automorphism group of the algebra A , using Harada's result [11] on the regular representation of A and the description of $\text{Aut}(A)$ given by Allen [2] in the case

when $\text{Aut}(A) \subseteq \Sigma_{n+1}$.

In chapters IV and V we determine $\text{Aut}(A)$ which, because of Allen's result [2], consists of showing that $\text{Aut}(A) \subseteq \Sigma_{n+1}$. The case $b = 0$ is dealt in chapter IV, while the case $b = a+c$ is dealt in chapter V. The treatment of the two cases is different, since for the case $b = 0$ we can identify A with a multiplicative subset A^* of an $n+1$ -dimensional algebra B having the same multiplication table as A , and it is simpler to work with A^* . In our method, no such identification is possible if $b \neq 0$, and hence calculations for the case $b = a+c$ are considerably more complicated.

If $b = 0$, since $c \neq 0$ the relation $a + (n-1)b = (q-1)c$ implies that $a \neq 0$. If $b = a+c$, by a suitable scaling down we can assume $c = n/q$ and $a = 1-c$ and hence once again $a \neq 0$. So in any case $a \neq 0$. Recently H. Suzuki [20] has developed a method to pass to an $n+1$ -dimensional algebra if $a \neq 0$, and the underlying field is the field of complex numbers. Hence for algebras over complex number field, his method covers both the cases dealt in our work, as well as algebras arising from many more doubly transitive groups.

It is hoped that in future one would be able to classify algebras for all finite simple groups and recover the groups from the automorphism groups of these algebras.

Harada [10] considered the 6-dimensional algebra A associated with the group $G = \text{PSL}(3,2)$ in the case $b = 0$. By determining all the idempotents of A , he was able to show that $\text{Aut}(A) \cong G$.

As a test case, we tried the same procedure for the 12-dimensional algebra A associated with the group $\text{PSL}(3,3)$. To determine the idempotents of A , one needs to solve a system of 12 quadratic equations in 12 unknowns. We solved this system on computer for the case when characteristic of K is 3. Having listed all the idempotents, it was not hard to show that $\text{Aut}(A) \cong \text{PSL}(3,3)$.

We remark, however, that this was only a test case and it convinced us that it is reasonable to expect that for $G = \text{PSL}(m,q)$, $\text{Aut}(A)$ will not be "too far away" from G . Our method to determine the automorphism group is absolutely computer-free.

In this thesis, the chapters are divided into sections, and the number of any result consists of the chapter number, the section number and the number of the result. For example, lemma 5.3.3 means the third lemma in section 3 of chapter V.

CHAPTER I
COMMUTATIVE ALGEBRAS ASSOCIATED WITH
DOUBLY TRANSITIVE PERMUTATION GROUPS AND
AUTOMORPHISM GROUPS OF THESE ALGEBRAS

§1. PERMUTATION GROUPS AND COMMUTATIVE ALGEBRAS

Definition 1.1.1: A finite dimensional vector-space V over a field K is said to be an algebra if V has a binary product which is K -linear with respect to each variable.

Remark 1.1.2: We do not require the binary product of V to be associative. In fact, algebras appearing in our work are never associative.

Definition 1.1.3: For an algebra V , we define the automorphism group of V , denoted by $\text{Aut}(V)$, to be the set

$$\text{Aut}(V) = \{\sigma \in \text{GL}(V) : (uv)^\sigma = u^\sigma v^\sigma \ \forall \ u, v \in V\}.$$

Harada [10] showed that any permutation group G gives rise to a G -invariant algebra A , so that G is isomorphic to a subgroup of $\text{Aut}(A)$. He classified all G -invariant commutative algebras for a doubly transitive permutation group G . In the remaining of this chapter we briefly discuss Harada's work. We mention most of the results without proof.

Let G be a permutation group on a set

$$\Omega = \{1, 2, \dots, n+1\}$$

and let V be the permutation module of G over a field K with basis $\{v_1, v_2, \dots, v_{n+1}\}$, where the permutation action is given by $v_i^g = v_{i^g}$ for all g in G , $1 \leq i \leq n+1$.

Let $u = v_1 + v_2 + \dots + v_{n+1}$ and $U = Ku$. U is a trivial submodule of V . Let $A = V/U$. Then A is an n -dimensional G -module. If we put $x_i = v_i + U$, $1 \leq i \leq n+1$, then $\{x_i : 1 \leq i \leq n+1\}$ generates A . Since $x_{n+1} = -x_1 - x_2 - \dots - x_n$, we can choose $\{x_i : 1 \leq i \leq n\}$ as a basis of A .

The tensor product $A \otimes_K A$ (to be hereafter denoted by $A \otimes A$) is also a G -module with the standard action $(a \otimes b)^g = a^g \otimes b^g$ for all g in G . Let θ be an isomorphism of $A \otimes A$ such that $\theta(x_i \otimes x_j) = x_j \otimes x_i$, $1 \leq i, j \leq n$. Then $\theta(x \otimes y) = y \otimes x$ for all x, y in A , hence θ does not depend on the choice of the basis. Moreover, $\theta^2 = 1$.

Let $S^2(A) = \{z \in A \otimes A : \theta(z) = z\}$. Then $S^2(A)$ has basis $\{x_i \otimes x_i, x_j \otimes x_k + x_k \otimes x_j : 1 \leq i \leq n, 1 \leq j < k \leq n\}$. Hence the dimension of $S^2(A)$ over K is $n(n+1)/2$. $S^2(A)$ is called the symmetric square of A .

Proposition 1.1.4: There exists a non trivial G -homomorphism ψ from $S^2(A)$ to A .

If the characteristic of K (to be hereafter denoted by $\text{ch}(K)$) is not equal to 2, $S^2(A)$ is a direct summand of $A \otimes A$ as a G -submodule. Consider the composition f of the three mappings

$$f : A \times A \xrightarrow{p} A \otimes A \xrightarrow{q} S^2(A) \xrightarrow{\psi} A$$

where $p(a,b) = a \otimes b$ for a,b in A , q is the projection $q(a \otimes b) = (a \otimes b + b \otimes a)/2$ and ψ is the mapping given by proposition 1.1.4.

Define $ab = f(a,b)$ for a,b in A . Then $f(a,b) = f(b,a)$ for all a,b in A , and $f(a,b)^g = f(a^g, b^g)$ for all g in G , hence we obtain a commutative G -invariant algebra structure on A . The binary product satisfies

$$\begin{aligned} x_i x_i &= (n-1)x_i, & 1 \leq i \leq n+1 \\ x_i x_j &= -(x_i + x_j), & 1 \leq i < j \leq n+1 \end{aligned} \quad (*)$$

Although $(*)$ is obtained under the assumption that $\text{ch}(K) \neq 2$, it is still valid for fields of characteristic 2. Hence A has at least one commutative G -invariant algebra structure over any field K .

Summarizing, we get

Theorem 1.1.5: Let G be a permutation group on a set $\Omega = \{1, 2, \dots, n+1\}$. Let $A = V/U$ be the n -dimensional G -module (constructed above) over a field K . Then A possesses at least one G -invariant commutative algebra structure given by

$$\begin{aligned} x_i x_i &= (n-1)x_i, & 1 \leq i \leq n+1 \\ x_i x_j &= -(x_i + x_j), & 1 \leq i < j \leq n+1 \end{aligned} \quad (*)$$

Remark 1.1.6: The multiplication by x_{n+1} is a consequence of the multiplication by the other x_i , since $x_{n+1} = -x_1 - x_2 - \dots - x_n$.

If the permutation action of G is triply transitive, then Harada [9] showed that up to scalar multiplication of basis elements, $(*)$ is the unique G -invariant commutative algebra structure on A , and if $\text{ch}(K) = 0$ or $\text{ch}(K) > n+1$, then $\text{Aut}(A) \cong \Sigma_{n+1}$, the symmetric group on $n+1$ letters. Allen [1] showed that if G is triply transitive, then

$$\text{Aut}(A) \cong \begin{cases} \Sigma_{n+1}, & \text{if } \text{ch}(K) = 0 \text{ or } \text{ch}(K) \nmid n+1 \\ K^{n-1} \cdot \text{GL}(n-1, K), & \text{if } \text{ch}(K) \mid n+1 \end{cases}$$

where $K^{n-1} \cdot \text{GL}(n-1, K)$ is a semidirect product of K^{n-1} , the $n-1$ dimensional vector space over K , and $\text{GL}(n-1, K)$, with natural action of $\text{GL}(n-1, K)$ on K^{n-1} .

§ 2. DOUBLY TRANSITIVE PERMUTATION GROUPS AND
COMMUTATIVE ALGEBRAS

We next turn our attention to a doubly transitive permutation group G , acting on a set of $n+1$ elements. Harada [10] showed that if G is not triply transitive, then A possesses, in general, more than one G -invariant commutative algebra structure, and the multiplication table is more complicated than (*). We first fix some notation.

G : a doubly transitive permutation group on a set $\Omega = \{1, 2, \dots, n+1\}$;

K : a field;

V : the permutation module of G over K , with basis $\{v_1, v_2, \dots, v_{n+1}\}$, such that $v_i^g = v_i$ $\forall g \in G, 1 \leq i \leq n+1$;

$G_{i,j}$: the pointwise stabilizer in G of $\{i, j\} \subset \Omega$;

$G_{i,j}^*$: the global stabilizer in G of $\{i, j\} \subset \Omega$,

that is, $G_{i,j}^* = \langle \tau \rangle G_{i,j}$, where $\tau \in G, \tau = (i \ j)\delta, \delta \in \Sigma_{\Omega \setminus \{i, j\}}$ (Σ_Γ denotes the symmetric group on the set Γ);

$\{\Omega(i, j; l) : 0 \leq l \leq k\}$: the set of all orbits of Ω under the action of $G_{i,j}^*$, $k+1$ being the number of these orbits. We choose notation so that $\Omega(i, j; 0) = \{i, j\}$ and $\Omega(i, j; l)^g = \Omega(i^g, j^g; l), g \in G, 0 \leq l \leq k$;

$r_l = |\Omega(i, j; l)|, 0 \leq l \leq k$;

$$u = v_1 + v_2 + \dots + v_{n+1};$$

$$U = Ku; \quad x_i = v_i + U, \quad 1 \leq i \leq n+1;$$

$$A = V/U;$$

$$\overline{\Omega}(i, j, 1) = \sum_{t \in \Omega(i, j, 1)} x_t;$$

Remark 1.2.1: $G_{i,j}^*$ does not depend on the choice of τ , since if τ_1 is another element of G interchanging i and j , then $\tau\tau_1^{-1} \in G_{i,j}$.

A is an n -dimensional G -module over K , generated by the set $\{x_i : 1 \leq i \leq n+1\}$. Since $x_{n+1} = -x_1 - x_2 - \dots - x_n$, we can choose the set $\{x_i : 1 \leq i \leq n\}$ as a basis of A over K . In the previous section we observed that A possesses at least one G -invariant commutative algebra structure. Harada [10] determined all G -invariant commutative algebra structures of A . If Ω has $k+1$ orbits under the action of $G_{i,j}^*$, then the algebra structure of A involves k independent parameters.

Lemma 1.2.2: We have

$$x_i x_i = a x_i, \quad 1 \leq i \leq n+1,$$

where a is a constant in K .

By renaming if necessary, we can assume that $0 \in \Omega(1, 2, k)$, and r_k is the largest among all r_1 's, $1 \leq l \leq k$.

Lemma 1.2.3: The following holds, provided $\text{ch}(K) \neq 2$,

$$x_i x_j = b(x_i + x_j) + \sum_{l=1}^{k-1} c_l \bar{\Omega}(i, j, l), \quad 1 \leq i < j \leq n+1$$

where $b, c_l, 1 \leq l \leq k-1$, are constants in K .

Lemma 1.2.4: The following holds, provided $\text{ch}(K) \neq 2$,

$$a + (n-1)b = \sum_{l=1}^{k-1} c_l r_l$$

Remark 1.2.5: Although in Harada [10] lemma 1.2.4 is proved for $\text{ch}(K) \neq 2$, it is not difficult to show that it is true for fields of arbitrary characteristic.

We now come to the main result of this section:

Theorem 1.2.6: Let G be a doubly transitive permutation group acting on a set $\Omega = \{1, 2, \dots, n+1\}$. Let A be a commutative (not necessarily associative) algebra over a field K with basis $\{x_1, x_2, \dots, x_n\}$. Assume that the product of A is defined as

$$\begin{aligned} x_i x_i &= ax_i, \quad 1 \leq i \leq n, \\ x_i x_j &= b(x_i + x_j) + \sum_{l=1}^{k-1} c_l \bar{\Omega}(i, j, l), \quad 1 \leq i < j \leq n, \end{aligned}$$

where $a, b, c_l \in K, 1 \leq l \leq k-1, a + (n-1)b = \sum_{l=1}^{k-1} c_l r_l$,

$x_{n+1} = -x_1 - x_2 - \dots - x_n$, and $r_l, \bar{\Omega}(i, j, l)$ being the same

as before. Then G preserves the product of A , that is, G is isomorphic to a subgroup of $\text{Aut}(A)$. Conversely, any G -invariant commutative algebra A has structure determined as above, provided $\text{ch}(K) \neq 2$.

Remark 1.2.7: There is a counterexample to theorem 1.2.6 if $\text{ch}(K) = 2$. But if all $G_{i,j}^*$ orbits of Ω are self paired, then the theorem also holds for fields of characteristic 2.

Corollary 1.2.8: If $\text{ch}(K) = 0$ or $\text{ch}(K) > n+1$, then the multiplicity of A in $S^2(A)$, as G -modules, is equal to the number of orbits of $G_{i,j}^*$ on $\Omega \setminus \{i,j\}$.

CHAPTER II
 COMMUTATIVE ALGEBRAS
 ASSOCIATED WITH $\text{PSL}(m,q)$, $m \geq 3$

§1. THE GROUP $\text{PSL}(m,q)$

Let $F = \text{GF}(q)$, a finite field of q elements, where q is a prime power. Let $\text{GL}(m,q)$ be the multiplicative group of all $m \times m$ nonsingular matrices with entries in F . $\text{GL}(m,q)$ is known as the general linear group of degree m over F . The special linear group $\text{SL}(m,q)$ is the subgroup of $\text{GL}(m,q)$ containing matrices of determinant 1. The projective special linear group $\text{PSL}(m,q)$ is the quotient group

$$\text{PSL}(m,q) = \text{SL}(m,q)/Z(\text{SL}(m,q)),$$

where $Z(\text{SL}(m,q))$ is the center of $\text{SL}(m,q)$.

It is well known (see Huppert [12], p.179) that

$$|\text{PSL}(m,q)| = \frac{(q^m-1)(q^m-q) \dots (q^m-q^{m-1})}{d(q-1)}$$

where $d = \text{gcd}(m, q-1)$.

Remark 2.1.1: $\text{PSL}(m,q)$ is simple except $m=2$, $q=2$ and $m=2$, $q=3$ (see Huppert [12], p.182).

§2. ACTION OF $PSL(m, q)$ ON $PG(m-1, q)$

Let $PG(m-1, q)$ be the $m-1$ dimensional projective space over F , that is, $PG(m-1, q)$ is the set of all 1-dimensional subspaces of the m -dimensional affine space F^m . $PG(m-1, q)$ has $(q^m-1)/(q-1)$ elements. The following result is well known and easy to prove (see Huppert [12], p.182).

Lemma 2.2.1: $PSL(m, q)$ acts as a doubly transitive permutation group on $PG(m-1, q)$.

Let $\Omega = \{1, 2, \dots, n+1\}$, where $n = \frac{q^m-1}{q-1} - 1 = \frac{q^m-q}{q-1}$.

We put $PG(m-1, q) = \{y_1, y_2, \dots, y_{n+1}\}$ with $i \in \Omega$ corresponding to $y_i \in PG(m-1, q)$. Choose $w_j \in F^m$ such that $y_j = Fw_j$, $1 \leq j \leq n+1$. We write $ry_i + sy_j$ for the 1-dimensional subspace generated by $rw_i + sw_j$, $r, s \in F$, $1 \leq i, j \leq n+1$. For $i, j \in \Omega$, $ri \oplus sj$ is defined to be the number $k \in \Omega$ such that $y_k = ry_i + sy_j$, $r, s \in F$.

Given $i, j \in \Omega$, let $L(i, j) = \{i, j, i \oplus j, \dots, i \oplus (q-1)j\}$. $L(i, j)$ is called the projective line containing i and j . Hence $|L(i, j)| = q+1$, and there are in all

$$\binom{q^m-1}{q-1} \setminus \binom{q+1}{2} = \frac{(q^m-1)(q^m-q)}{(q^2-1)(q^2-q)}$$

such lines. It is an easy observation that if $k, l \in L(i, j)$, then $L(k, l) = L(i, j)$.

We fix some notation.

$$L(i', j) = L(i, j) \setminus \{i\}.$$

$$L(i, j') = L(i, j) \setminus \{j\}.$$

$$L(i', j') = L(i, j) \setminus \{i, j\}.$$

We have taken the sketch of the proof of the next lemma and the two remarks following it from Harada [11].

Lemma 2.2.2: Let $G = \text{PSL}(m, q)$, $m \geq 3$. Let $G_{i,j}^*$ be the global stabilizer of $\{i, j\} \subset \Omega$. Then the orbit lengths of $\Omega \setminus \{i, j\}$ under the action of $G_{i,j}^*$ are $q-1$ and $n-q$.

Proof: Since G is doubly transitive on Ω , we can choose $i=1$ and $j=2$, where $1 = Fw_1$, $2 = Fw_2$, $w_1 = (1, 0, 0, \dots, 0)$, $w_2 = (0, 1, 0, \dots, 0)$, $w_1, w_2 \in F^m$. (we identify $i \in \Omega$ with $y_i \in \text{PG}(m-1, q)$). Then the stabilizer $G_{i,j}^\#$ of the points i and j in $G^\# = \text{SL}(m, q)$ consists of matrices T of the type

$$T = \begin{pmatrix} \mu & 0 & \underline{0} \\ 0 & v & \underline{0} \\ \hline & & \\ & B & C \end{pmatrix}$$

where $\mu, v \in F \setminus \{0\}$, $\underline{0}$ is a $1 \times m-2$ zero matrix, and B, C are $m-2 \times 2$ and $m-2 \times m-2$ matrices respectively. We

also have $\mu \nu \det C = 1$. Let $L(1,2)$ be the projective line containing 1 and 2. Then

$$L(1',2') = \{(1,r,0, \dots, 0) : r \in F, r \neq 0\}.$$

It is easy to see that $G_{1,2}^\#$ is transitive on $L(1',2')$.

Assume next that not all of $\omega_3, \omega_4, \dots, \omega_m$ are zero, and let D be a matrix of the form

$$D = \left(\begin{array}{cc|cccc} \mu & 0 & & & & \\ 0 & \nu & & & & \\ \hline & & \underline{0} & & & \\ \omega_1 & \omega_2 & \omega_3 & \dots & \omega_m & \\ \hline & & \underline{0} & & (*) & \end{array} \right)$$

where $\underline{0}$ is a zero matrix of appropriate size. We choose $(*)$ suitably so that

$$\det D = \mu \nu \det \begin{pmatrix} \omega_3 & \dots & \omega_m \\ (*) \end{pmatrix} = 1.$$

Thus $G_{1,2}^\#$ has at most two orbits on $\Omega \setminus \{1,2\}$. Since $L(1',2')$ is obviously an orbit, the remaining $n-q$ points also form an orbit. This proves the orbit length structure of $\Omega \setminus \{1,2\}$ under the action of $G_{1,2}^\#$. Passing to the quotient, the same result holds for $G = \text{PSL}(m,q)$.

Remark 2.2.3: If $\text{PFL}(m,q)$ is the group of all projective semi-linear transformations on Ω , then any group G such that $\text{PSL}(m,q) \subseteq G \subseteq \text{PFL}(m,q)$ possesses the same orbit structure.

Remark 2.2.4: If $m \geq 3$, the global stabilizer $G_{i,j}^*$ has the same orbit lengths on $\Omega \setminus \{i,j\}$ as the pointwise stabilizer $G_{i,j}$, that is, orbits of Ω are 'self-paired' under the action of $G_{i,j}^*$. Hence theorem 1.2.6 holds for fields of any characteristic if $G = \text{PSL}(m,q)$, $m \geq 3$. But if $G = \text{PSL}(2,q)$ and q is odd, then $G_{i,j}^*$ is transitive on $\Omega \setminus \{i,j\}$ if $(q-1)/2$ is odd, while $G_{i,j}^*$ has two orbits, each of length $(q-1)/2$ if $(q-1)/2$ is even. On the other hand, in both cases $G_{i,j}$ has exactly two orbits, each of length $(q-1)/2$. If G is a group such that $\text{PGL}(2,q) \subseteq G \subseteq \text{P}\Gamma\text{L}(2,q)$, then $G_{i,j}$ is transitive on $\Omega \setminus \{i,j\}$ for all cases. Note that $\text{PSL}(2,q) = \text{PGL}(2,q)$ if q is even.

§3. THE ALGEBRA A

From now on we let G to be the group $\text{PSL}(m,q)$, $m \geq 3$. Let A be the commutative G -invariant algebra obtained from G as described in chapter II. Then the number k of orbits of $G_{i,j}^*$ is 2, and from theorem 1.2.6 we get that the algebra structure is given by

$$\begin{aligned} x_i x_i &= a x_i, & 1 \leq i \leq n+1, \\ x_i x_j &= b(x_i + x_j) + c \sum_{k \in L(i',j')} x_k, & 1 \leq i < j \leq n+1, \end{aligned}$$

with $a + (n-1)b = (q-1)c$, $a, b, c \in K$.

CHAPTER III
AUTOMORPHISM GROUP OF THE ALGEBRA A
ASSOCIATED WITH $PSL(m,q)$, $m \geq 3$

§1. THE ALGEBRA A

Let A be the algebra associated with $PSL(m,q)$, as described in chapters I and II. A is a vector space of dimension n over a field K, where $n = (q^m - q)/(q - 1)$. Let $\{x_1, x_2, \dots, x_n\}$ be a basis of A over K and let $x_{n+1} = -x_1 - x_2 - \dots - x_n$. Then the algebra multiplication of A is given by

$$\begin{aligned} x_i x_i &= ax_i, \quad 1 \leq i \leq n+1 \\ x_i x_j &= b(x_i + x_j) + c \sum_{k \in L(i', j')} x_k, \quad 1 \leq i < j \leq n \end{aligned} \quad (3.1)$$

with $a + (n-1)b = (q-1)c$, $a, b, c \in K$.

§2. THE REGULAR REPRESENTATION OF A

Let $\rho : A \longrightarrow \text{End}_K(A)$ be the regular representation of A, given by $\rho(x) = \rho_x$, $x \in A$, where

$$\rho_x(y) = xy, \quad y \in A.$$

Harada [11] showed that the characteristic polynomial $\chi(X)$ of ρ_{x_i} , $1 \leq i \leq n+1$, is

$$\chi(X) = (X-a)(X-b+c)^{n-\frac{n}{q}}(X-b-(q-1)c)^{\frac{n}{q}-1}.$$

He further showed that the minimal polynomial $m(X)$ of

$$p_x \quad m(X) = \begin{cases} (X-a)(X-b), & \text{if } c = 0 \\ (X-b+c)(X-b-(q-1)c), & \text{if } b(a+c-b) = 0 \\ (X-a)(X-b+c)(X-b-(q-1)c), & \text{otherwise.} \end{cases}$$

As already mentioned, if $c = 0$ then, ~~otherwise.~~

As already mentioned, if $c = 0$ then

$$\text{Aut}(A) \cong \begin{cases} \Sigma_{n+1}, & \text{if } \text{ch}(K) = 0 \text{ or } \text{ch}(K) \nmid n+1 \\ K^{n-1} \cdot \text{GL}(n-1, K), & \text{if } \text{ch}(K) \mid n+1 \end{cases}$$

In this thesis we consider the case

$$b(a+c-b) = 0, \quad c \neq 0,$$

and determine $\text{Aut}(A)$ under certain restrictions on the characteristic of K . The case $b = 0$ is treated in chapter IV, and the case $b = a+c$ is treated in chapter V.

If $b(a+c-b) = 0$, the minimal polynomial $m(X)$ is given by

$$\begin{aligned} m(X) &= (X-b+c)(X-b-(q-1)c) \\ &= X^2 - (2b+(q-2)c)X - ((q-1)c^2 - (q-2)bc - b^2). \end{aligned}$$

Therefore $\forall x_i, 1 \leq i \leq n+1, \forall x \in A$,

$$x_i(x_i x) = (2b+(q-2)c)x_i x + ((q-1)c^2 - (q-2)bc - b^2)x.$$

Hence if $\sigma \in \text{Aut}(A)$,

$$\begin{aligned} \sigma(x_i)(\sigma(x_i)\sigma(x)) &= (2b+(q-2)c)\sigma(x_i)\sigma(x) + \\ &\quad ((q-1)c^2 - (q-2)bc - b^2)\sigma(x). \end{aligned}$$

Since $\sigma(x)$ runs over all elements of A , we get that

$\forall \sigma \in \text{Aut}(A), \forall x \in A, \text{ and } \forall x_i, 1 \leq i \leq n+1,$

$$\sigma(x_i)(\sigma(x_i)x) = (2b+(q-2)c)\sigma(x_i)x + ((q-1)c^2-(q-2)bc-b^2)x \quad (3.2)$$

§3. THE AUTOMORPHISM GROUP OF A

Let V be a vector space of dimension m over a field F . A map $T : V \longrightarrow V$ is called a semi-linear transformation of V if

$$T(v_1+v_2) = T(v_1) + T(v_2), \quad \forall v_1, v_2 \in V,$$

$T(\lambda v) = \theta(\lambda)T(v), \quad \forall \lambda \in F, \forall v \in V$, where θ is an automorphism of F .

The set of all bijective semi-linear transformations forms a group, denoted by $\Gamma L(V)$ or $\Gamma L(m, F)$. If $F = GF(q)$, a field of q elements, we write $\Gamma L(m, q)$ for $\Gamma L(V)$.

The following results about $\Gamma L(V)$ are well known and we mention them without proof.

Let $\{v_1, v_2, \dots, v_m\}$ be a basis of V over F .

Lemma 3.3.1: Let $T \in \Gamma L(V)$ and let θ_T be the automorphism of F determined by T . Then $\exists T^* \in GL(V)$ such that $\forall v \in V, v = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_m v_m,$

$$T(v) = T^*(\theta_T(\lambda_1)v_1 + \theta_T(\lambda_2)v_2 + \dots + \theta_T(\lambda_m)v_m).$$

Lemma 3.3.2: Let $\theta \in \text{Aut}(F)$. Define $T_\theta : V \longrightarrow V$ as follows:

$$T_\theta(v) = \theta(\lambda_1)v_1 + \theta(\lambda_2)v_2 + \dots + \theta(\lambda_m)v_m,$$

where $v \in V$, $v = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_m v_m$. Then $T_\theta \in \text{FL}(V)$.

From lemmas 3.3.1 and 3.3.2 we get that

$$\text{FL}(V) = \{T^* T_\theta : \theta \in \text{Aut}(F), T^* \in \text{GL}(V)\}$$

Hence $\text{FL}(V)$ is a semidirect product of $\langle T_\theta : \theta \in \text{Aut}(F) \rangle$ and $\text{GL}(V)$. If $(t_{i,j})$ is the matrix of $T^* \in \text{GL}(V)$, then $(\theta(t_{i,j}))$ is the matrix of $T_\theta^{-1} T^* T_\theta \in \text{GL}(V)$. Hence $\text{GL}(V)$ is a normal subgroup of $\text{FL}(V)$ and $\text{FL}(V)/\text{GL}(V) \cong \text{Aut}(F)$.

If $F = \text{GF}(q)$, a finite field of q elements, and $q = p^r$, where p is a prime, then $\text{Aut}(F) \cong \mathbb{Z}/r\mathbb{Z}$, a cyclic group of order r . Hence

$$|\text{FL}(m,q)| = r|\text{GL}(m,q)|$$

$\text{FL}(V)$ acts on $\text{PG}(m-1, V)$, the $m-1$ dimensional projective space, in a natural way. If $Z(V)$ is the set of all $m \times m$ non zero scalar transformations on V , then $Z(V)$ is the kernel of the action of $\text{FL}(V)$ on $\text{PG}(m-1, V)$. Let $\text{PFL}(V)$ be the quotient group

$$\text{PFL}(V) = \text{FL}(V)/Z(V).$$

$\text{PFL}(V)$ is called the projective semi-linear group of V . As before, if $F = \text{GF}(q)$, we write $\text{PFL}(m,q)$ for $\text{PFL}(V)$.

$$|\text{PFL}(m,q)| = |\text{FL}(m,q)|/(q-1) = rd|\text{PSL}(m,q)|,$$

where $q = p^r$ and $d = \gcd(m, q-1)$. Therefore the groups

$\text{PSL}(m, q)$ and $\text{PFL}(m, q)$ are isomorphic if and only if $r=1$, that is, q is a prime and $\gcd(m, q-1) = 1$.

We have taken the following result from Allen [2]

Theorem 3.3.3: If $c \neq 0$, then $\text{Aut}(A) \cap \Sigma_{n+1} \cong \text{PFL}(m, q)$.

Proof: For i, j in Ω , $i \neq j$,

$$x_i x_j = b(x_i + x_j) + c \sum_{k \in L(i', j')} x_k$$

Let $\sigma \in \text{Aut}(A) \cap \Sigma_{n+1}$. Then $\sigma(x_i) = x_{\theta(i)}$, $1 \leq i \leq n+1$, where θ^{-1} is the permutation in Σ_{n+1} inducing σ . Comparing $\sigma(x_i x_j)$ with $\sigma(x_i) \sigma(x_j)$ we see that

$$b(x_{\theta(i)} + x_{\theta(j)}) + c \sum_{k \in L(i', j')} x_{\theta(k)} = b(x_{\theta(i)} + x_{\theta(j)}) + c \sum_{l \in L(\theta(i)', \theta(j)')} x_l$$

Therefore we get that if $k \in L(i', j')$, then

$\theta(k) \in L(\theta(i)', \theta(j)')$. By the fundamental theorem of

projective geometry (see Artin [3], p.88) there is a

semi-linear transformation of F^m which induces θ .

Conversely, any semi-linear transformation of F^m determines an element of $\text{Aut}(A) \cap \Sigma_{n+1}$. Since

$\text{FL}(m, q) \cong \text{GL}(m, q).Z/rZ$, where $q = p^r$ and the kernel of the epimorphism $\text{GL}(m, q).Z/rZ \longrightarrow \text{Aut}(A) \cap \Sigma_{n+1}$

$$T \longrightarrow "x_i \longrightarrow x_{T^{-1}(i)}"$$

is the set of non zero scalar matrices, we get

$$\text{PFL}(m, q) \cong \text{Aut}(A) \cap \Sigma_{n+1}.$$

Corollary 3.3.4: If $c \neq 0$ and $\text{Aut}(A) \subseteq \Sigma_{n+1}$, then
 $\text{Aut}(A) \cong \text{PFL}(m, q)$.

CHAPTER IV
 DETERMINATION OF THE AUTOMORPHISM GROUP
 OF A IN THE CASE $b = 0$

Throughout this chapter we assume that $q-1 \neq 0$ in K , $q+1 \neq 0$ in K and $n+1 \neq 0$ in K .

§1. THE ALGEBRA A

Since $b=0$, from $a+(n-1)b = (q-1)c$ we get $a = (q-1)c$. Since $c \neq 0$, without loss of generality we can assume $a=1$, $c=1/(q-1)$. Therefore the multiplication in A becomes

$$\begin{aligned} x_i x_i &= x_i, & 1 \leq i \leq n+1 \\ x_i x_j &= \frac{1}{q-1} \sum_{k \in L(i', j')} x_k, & 1 \leq i < j \leq n+1 \end{aligned}$$

§2. THE NEW ALGEBRA B, ITS SUBSET A^*

Lemma 4.2.1: Let V be an n -dimensional vector space over a field K , $\text{ch}(K) \nmid n+1$. Let $\{v_1, v_2, \dots, v_n\}$ be a basis of V , and let $v_{n+1} = -v_1 - v_2 - \dots - v_n$. Suppose $v \in V$, $v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$. If we write $v = b_1 v_1 + b_2 v_2 + \dots + b_{n+1} v_{n+1}$, with $b_1 + b_2 + \dots + b_{n+1} = \lambda$, where λ is a fixed element of K , then $b_1, b_2, \dots, b_{n+1}$ are uniquely determined.

Proof:

$$\sum_{i=1}^{n+1} b_i v_i = \sum_{i=1}^n (b_i - b_{n+1}) v_i$$

Therefore $b_i - b_{n+1} = a_i$, $1 \leq i \leq n$

Putting $b_{n+1} = \lambda - b_1 - b_2 - \dots - b_n$ (4.1)

we get $b_i - (\lambda - \sum_{j=1}^n b_j) = a_i$, $1 \leq i \leq n$,

or $2b_i + \sum_{\substack{j=1 \\ j \neq i}}^n b_j = a_i + \lambda$, $1 \leq i \leq n$ (4.2)

Subtracting i -th equation ($i \neq 1$) of (4.2) from first, we get $b_1 - b_i = a_1 - a_i$, $2 \leq i \leq n$,

or $b_i = b_1 - (a_1 - a_i)$, $2 \leq i \leq n$ (4.3)

Putting in the first equation of (4.2), we get

$$2b_1 + \sum_{i=2}^n (b_1 - (a_1 - a_i)) = a_1 + \lambda$$

or $(n+1)b_1 - (n-1)a_1 + \sum_{i=2}^n a_i = a_1 + \lambda$,

or $(n+1)b_1 = na_1 - \sum_{i=2}^n a_i + \lambda$

Since $\text{ch}(K) \nmid n+1$, $b_1 = \frac{1}{n+1}(na_1 - \sum_{i=2}^n a_i + \lambda)$

Putting the value of b_1 in equation (4.3), we get

b_i , $2 \leq i \leq n$. b_{n+1} is then determined from equation (4.1).

Let B be an $n+1$ -dimensional algebra over K with basis $\{w_1, w_2, \dots, w_{n+1}\}$, and the product given by

$$w_i w_i = w_i, \quad 1 \leq i \leq n+1,$$

$$w_i w_j = \frac{1}{q-1} \sum_{k \in L(i', j')} w_k, \quad 1 \leq i < j \leq n+1$$

Define $S : B \longrightarrow K$ by

$$S(a_1 w_1 + a_2 w_2 + \dots + a_{n+1} w_{n+1}) = a_1 + a_2 + \dots + a_{n+1}$$

Let $A^* = \{v \in B : S(v) = 1\}$.

Lemma 4.2.2: A^* is a multiplicatively closed set, that is, $v_1^*, v_2^* \in A^*$ implies $v_1^* v_2^* \in A^*$.

$$\text{Proof: Let } v_1^* = \sum_{i=1}^{n+1} a_i w_i, \quad v_2^* = \sum_{i=1}^{n+1} b_i w_i$$

$$\begin{aligned} v_1^* v_2^* &= \sum_{i=1}^{n+1} a_i b_i w_i^2 + \sum_{\substack{i, j=1 \\ i \neq j}}^{n+1} a_i b_j w_i w_j \\ &= \sum_{i=1}^{n+1} a_i b_i w_i + \sum_{\substack{i, j=1 \\ i \neq j}}^{n+1} a_i b_j \left(\frac{1}{q-1} \sum_{k \in L(i', j')} w_k \right) \end{aligned}$$

Since $|L(i', j')| = q-1$, $a_i b_j$ gets added $q-1$ times in $S(v_1^* v_2^*)$. Hence

$$\begin{aligned} S(v_1^* v_2^*) &= \sum_{i=1}^{n+1} a_i b_i + \sum_{\substack{i, j=1 \\ i \neq j}}^{n+1} a_i b_j = \sum_{i, j=1}^{n+1} a_i b_j \\ &= \left(\sum_{i=1}^{n+1} a_i \right) \left(\sum_{j=1}^{n+1} b_j \right) = S(v_1^*) S(v_2^*) = 1 \end{aligned}$$

Therefore $v_1^* v_2^* \in A^*$.

By lemma 4.2.1 A is in one-to-one correspondence with A^* (for $\lambda=1$) and this correspondence clearly preserves multiplication. Hence multiplicatively we can identify A with A^* , that is, we can express every element of A uniquely as $a_1x_1 + a_2x_2 + \dots + a_{n+1}x_{n+1}$, with $a_1 + a_2 + \dots + a_{n+1} = 1$, and we can compare coefficients on multiplying. With this in mind, multiplication in A is given by

$$\begin{aligned}
 \left(\sum_{i=1}^{n+1} a_i x_i \right) \left(\sum_{i=1}^{n+1} b_i x_i \right) &= \sum_{i=1}^{n+1} a_i b_i x_i^2 + \sum_{\substack{i,j=1 \\ i \neq j}}^{n+1} a_i b_j x_i x_j \\
 &= \sum_{i=1}^{n+1} a_i b_i x_i + \frac{1}{q-1} \sum_{\substack{i,j=1 \\ i \neq j}}^{n+1} a_i b_j \left(\sum_{k \in L(i,j)} x_k \right) \\
 &= \sum_{i=1}^{n+1} a_i b_i + \frac{1}{q-1} \sum_{L \ni i} \left(\sum_{\substack{k,l \in L \setminus \{i\} \\ k \neq l}} a_k b_l \right) x_i
 \end{aligned}$$

Hence

$$\left(\sum_{i=1}^{n+1} a_i x_i \right) \left(\sum_{i=1}^{n+1} b_i x_i \right) = \sum_{i=1}^{n+1} a_i b_i + \frac{1}{q-1} \sum_{L \ni i} \left(\sum_{\substack{k,l \in L \setminus \{i\} \\ k \neq l}} a_k b_l \right) x_i \quad (4.4)$$

§3. THE RELATION OBTAINED FROM THE MINIMAL POLYNOMIAL

As mentioned in chapter III, the minimal polynomial of the multiplication by x_i , $1 \leq i \leq n+1$, is given by

$$m(X) = (X-b+c)(X-b-(q-1)c), \text{ if } b(a+c-b) = 0.$$

Therefore, if $b=0$, $c=1/(q-1)$, we get

$$m(X) = (X + \frac{1}{q-1})(X-1) = X^2 - \frac{q-2}{q-1} X - \frac{1}{q-1}$$

Hence, $\forall x \in A, \forall x_i, 1 \leq i \leq n+1$,

$$x_i(x_i x) = \frac{q-2}{q-1} x_i x + \frac{1}{q-1} x \quad (4.5)$$

Remark 4.3.1: Equation (4.5), which is key to the calculation of $\text{Aut}(A)$, was first observed by S.K.Wong for the special cases $G = \text{PSL}(3,2)$ and $G = \text{PSL}(3,3)$, and is easy to obtain from the algebra multiplication. The study of the case $b = a + c$ became possible after Harada [11] generalized it to the minimal polynomial. We next give our original proof for the result.

Lemma 4.3.2 (Wong): $x_i(x_i x) = \frac{q-2}{q-1} x_i x + \frac{1}{q-1} x$, $\forall x \in A, \forall x_i, 1 \leq i \leq n+1$.

Proof: For $i \neq j$, $x_i x_j = \frac{1}{q-1} \sum_{k \in L(i', j')} x_k$

Therefore $x_i(x_i x_j) = \frac{1}{q-1} \left(\sum_{k \in L(i', j')} x_i x_k \right)$

$$\text{or } x_i(x_i x_j) = \frac{1}{(q-1)^2} \left(\sum_{k \in L(i', j')} \left(\sum_{l \in L(i', k')} x_l \right) \right)$$

But $k \in L(i, j)$ and $k \neq j$. Therefore x_j appears in the last summation. Hence

$$\begin{aligned} x_i(x_i x_j) &= \frac{1}{(q-1)^2} \left(\sum_{k \in L(i', j')} (x_j + \sum_{\substack{l \in L(i', k') \\ l \neq j}} x_l) \right) \\ &= \frac{1}{(q-1)^2} \left((q-1)x_j + \sum_{k \in L(i', j')} \sum_{\substack{l \in L(i', k') \\ l \neq j}} x_l \right) \\ &= \frac{1}{q-1} x_j + \frac{q-2}{q-1} \sum_{k \in L(i', j')} x_k, \end{aligned}$$

since interchanging the summation we add all terms $q-2$ times. Hence for $i \neq j$,

$$x_i(x_i x_j) = \frac{1}{q-1} x_j + \frac{q-2}{q-1} x_i x_j.$$

But this relation is true even if $i=j$. Hence

$$x_i(x_i x_j) = \frac{q-2}{q-1} x_i x_j + \frac{1}{q-1} x_j, \quad 1 \leq i, j \leq n+1$$

Hence $\forall x \in A, \forall x_i, 1 \leq i \leq n+1$,

$$x_i(x_i x) = \frac{q-2}{q-1} x_i x + \frac{1}{q-1} x$$

Let $\sigma \in \text{Aut}(A)$. Applying σ to equation (4.5), we get

$$\sigma(x_i)(\sigma(x_i)\sigma(x)) = \frac{q-2}{q-1} \sigma(x_i)\sigma(x) + \frac{1}{q-1} \sigma(x)$$

Since $\sigma(x)$ runs over all elements of A , we get that

$\forall x \in A, \forall x_i, 1 \leq i \leq n+1$,

$$\sigma(x_i)(\sigma(x_i)x) = \frac{q-2}{q-1} \sigma(x_i)x + \frac{1}{q-1} x. \quad (4.6)$$

§4. CALCULATION OF THE AUTOMORPHISM GROUP OF A

We now proceed to show that $\text{Aut}(A)$ permutes the set $\{x_1, x_2, \dots, x_{n+1}\}$, that is, $\sigma(x_1) \in \{x_1, x_2, \dots, x_{n+1}\}$ $\forall \sigma \in \text{Aut}(A)$.

Let $\sigma(x_1) = a_1 x_1 + a_2 x_2 + \dots + a_{n+1} x_{n+1}$, such that $a_1 + a_2 + \dots + a_{n+1} = 1$.

For $i \neq j$, let $S(i, j) = \sum_{k \in L(i', j')} a_k$, $T(i, j) = \sum_{k \in L(i', j')} a_k^2$

For the remaining of this chapter, Σ stands for $\sum_{i=1}^{n+1}$.

Since $x_1^2 = x_1$, $\sigma(x_1^2) = \sigma(x_1)$, or $(\sum_i a_i x_i)^2 = \sum_i a_i x_i$

Putting $a_i = b_i$ in equation (4.4), we get

$$\sum_i (a_i^2 + \frac{1}{q-1} \sum_{L \ni i} (\sum_{\substack{k, l \in L \setminus \{i\} \\ k \neq l}} a_k a_l)) x_i = \sum_i a_i x_i$$

Hence $(q-1)a_i^2 + \sum_{L \ni i} (\sum_{\substack{k, l \in L \setminus \{i\} \\ k \neq l}} a_k a_l) = (q-1)a_i$, $1 \leq i \leq n+1$

or $(q-1)a_i^2 + \sum_{j \neq i} a_j S(i, j) = (q-1)a_i$, $1 \leq i \leq n+1$ (4.7)

We put $i=1$ and $x = x_r$, $1 \leq r \leq n+1$, in equation (4.6) to get

$$\sigma(x_1)(\sigma(x_1)x_r) = \frac{q-2}{q-1} \sigma(x_1)x_r + \frac{1}{q-1} x_r \quad (4.8)$$

Let $\sigma(x_1)x_r = \frac{1}{q-1} \sum_i b_i(r)x_i$ with $\sum_i b_i(r) = (q-1)$,

$1 \leq r \leq n+1$.

Lemma 4.4.1: $b_r(r) = (q-1)a_r$, and for $i \neq r$,

$$b_i(r) = \sum_{k \in L(i', r')} a_k = S(i, r), \quad 1 \leq r \leq n+1.$$

$$\text{Proof: } \frac{1}{q-1} \sum_i b_i(r)x_i = \sigma(x_1)x_r = \left(\sum_i a_i x_i \right) x_r$$

$$= a_r x_r + \sum_{i \neq r} a_i x_i x_r$$

$$= a_r x_r + \sum_{i \neq r} a_i \frac{1}{q-1} \left(\sum_{k \in L(i', r')} x_k \right).$$

$$= \sum_i \left(a_i + \frac{1}{q-1} \sum_{k \in L(i', r')} a_k \right) x_i$$

Hence $b_r(r) = (q-1)a_r$, and for $i \neq r$, $b_i(r) = \sum_{k \in L(i', r')} a_k$

We now put $r = 1$ to get

$$\sigma(x_1)x_1 = \frac{1}{q-1} \sum_i b_i(1)x_i, \text{ with } b_1(1) = (q-1)a_1,$$

$b_i(1) = S(i, 1)$ for $i \neq 1$, $1 \leq i \leq n+1$. Putting in equation (4.6) we get

$$\left(\sum_i a_i x_i \right) \frac{1}{q-1} \left(\sum_j b_j(1)x_j \right) = \frac{q-2}{(q-1)^2} \sum_j b_j(1)x_j + \frac{1}{q-1} x_1$$

$$\text{or } \left(\sum_i a_i x_i \right) \left(\sum_j b_j(1)x_j \right) = \frac{q-2}{q-1} \sum_j b_j(1)x_j + x_1.$$

Using equation (4.4) we get

$$\sum_i \left(a_i b_i(1) + \frac{1}{q-1} \sum_{L \ni i} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k \neq l}} a_k b_l(1) \right) \right) x_i = \frac{q-2}{q-1} \sum_i b_i(1)x_i + x_1$$

$$\text{or } \sum_i ((q-1)a_i b_i(1) + \sum_{L \ni i} \sum_{\substack{k, l \in L \setminus \{i\} \\ k \neq l}} a_k b_l(1)) x_i = (q-2) \sum_i b_i(1) x_i + (q-1) x_1$$

$$\text{or } \sum_i ((q-1)a_i b_i(1) + \sum_{j \neq i} a_j (\sum_{k \in L(i', j')} b_k(1))) x_i = (q-2) \sum_i b_i(1) x_i + (q-1) x_1$$

Comparing the coefficient of x_2 , we get

$$(q-1)a_2 b_2(1) + \sum_{j \neq 2} a_j (\sum_{k \in L(2', j')} b_k(1)) = (q-2)b_2(1)$$

$$\text{or } (q-1)a_2 S(1,2) + \sum_{j \neq 2} a_j (\sum_{k \in L(2', j')} S(1,k)) = (q-2)S(1,2) \quad (4.9)$$

where $S(1,1) = b_1(1) = (q-1)a_1$. Equation (4.9) can be written as

$$\begin{aligned} (q-1)a_2 S(1,2) + \sum_{j \in L(1,2')} a_j (\sum_{k \in L(2', j')} S(1,k)) + \\ \sum_{j \notin L(1,2)} a_j (\sum_{k \in L(2', j')} S(1,k)) = (q-2)S(1,2) \end{aligned}$$

By rearranging the terms, it is easy to see that

$$\sum_{j \notin L(1,2)} a_j (\sum_{k \in L(2', j')} S(1,k)) = \sum_{j \notin L(1,2)} a_j (\sum_{k \in L(1', 2')} S(j,k))$$

$$\text{Also, } \sum_{j \in L(1,2')} a_j (\sum_{k \in L(2', j')} S(1,k)) =$$

$$a_1 \sum_{k \in L(1', 2')} S(1,k) + \sum_{j \in L(1', 2')} a_j (\sum_{k \in L(2', j')} S(1,k)) = a_1 \sum_{k \in L(1', 2')} S(1,k)$$

$$+ \sum_{j \in L(1', 2')} a_j ((q-1)a_1 + (q-2)a_2 + (q-2)a_j + (q-3) \sum_{\substack{k \in L(1', 2') \\ k \neq j}} a_k)$$

$$= a_1 \sum_{k \in L(1', 2')} S(1, k) + (q-1)a_1 S(1, 2) + (q-2)a_2 S(1, 2) + \\ (q-2)T(1, 2) + (q-3) \sum_{\substack{j, k \in L(1', 2') \\ j \neq k}} a_j a_k$$

Therefore equation (4.9) becomes

$$(q-1)a_2 S(1, 2) + a_1 \sum_{k \in L(1', 2')} S(1, k) + (q-1)a_1 S(1, 2) + \\ (q-2)a_2 S(1, 2) + (q-2)T(1, 2) + (q-3) \sum_{\substack{j, k \in L(1', 2') \\ j \neq k}} a_j a_k + \\ \sum_{j \notin L(1, 2)} a_j \left(\sum_{k \in L(1', 2')} S(j, k) \right) = (q-2)S(1, 2) \quad (4.10)$$

Now consider equation (4.7), viz.,

$$(q-1)a_i^2 + \sum_{j \neq i} a_j S(i, j) = (q-1)a_i, \quad 1 \leq i \leq n+1$$

Summing over all $i \in L(1', 2')$, we get

$$(q-1)T(1, 2) + \sum_{i \in L(1', 2')} \left(\sum_{j \neq i} a_j S(i, j) \right) = (q-1)S(1, 2)$$

Rearranging the terms, we get

$$(q-1)T(1, 2) + a_1 \sum_{k \in L(1', 2')} S(1, k) + a_2 \sum_{k \in L(1', 2')} S(2, k) + \\ \sum_{i \in L(1', 2')} a_i \left(\sum_{\substack{j \in L(1', 2') \\ j \neq i}} S(i, j) \right) + \sum_{j \notin L(1, 2)} a_j \left(\sum_{k \in L(1', 2')} S(j, k) \right) = \\ (q-1)S(1, 2) \quad (4.11)$$

Subtracting (4.10) from (4.11), we get

$$\begin{aligned}
 T(1,2) + a_2 \sum_{k \in L(1',2')} S(2,k) + \sum_{i \in L(1',2')} a_i \left(\sum_{\substack{j \in L(1',2') \\ j \neq i}} S(i,j) \right) - \\
 (q-1)a_2 S(1,2) - (q-1)a_1 S(1,2) - (q-2)a_2 S(1,2) - \\
 (q-3) \sum_{\substack{j,k \in L(1',2') \\ j \neq k}} a_j a_k = S(1,2) \quad (4.12)
 \end{aligned}$$

But $a_2 \sum_{k \in L(1',2')} S(2,k) = (q-1)a_1 a_2 + (q-2)a_2 S(1,2)$. Also by an easy rearrangement,

$$\begin{aligned}
 \sum_{i \in L(1',2')} a_i \left(\sum_{\substack{j \in L(1',2') \\ j \neq i}} S(i,j) \right) &= (q-2)a_1 S(1,2) + \\
 &\quad (q-2)a_2 S(1,2) + (q-3) \sum_{\substack{j,k \in L(1',2') \\ j \neq k}} a_j a_k
 \end{aligned}$$

Substituting in (4.12), we get

$$\begin{aligned}
 T(1,2) + (q-1)a_1 a_2 + (q-2)a_2 S(1,2) + (q-2)a_1 S(1,2) + \\
 (q-2)a_2 S(1,2) + (q-3) \sum_{\substack{j,k \in L(1',2') \\ j \neq k}} a_j a_k - (q-2)a_2 S(1,2) - \\
 (q-1)a_1 S(1,2) - (q-1)a_2 S(1,2) - (q-3) \sum_{\substack{j,k \in L(1',2') \\ j \neq k}} a_j a_k = S(1,2)
 \end{aligned}$$

$$\text{or } T(1,2) + (q-1)a_1 a_2 - a_1 S(1,2) - a_2 S(1,2) = S(1,2) \quad (4.13)$$

We obtained equation (4.13) by putting $r = 1$ in equation (4.8) and comparing the coefficient of x_2 . We could have started with any $r \in L(1,2)$ and compared the

coefficient of any x_s , $s \in L(1,2)$, $s \neq r$, to get an equation like (4.13). Hence we get $\binom{q+1}{2}$ equations

$$T(i,j) + (q-1)a_i a_j = (a_i + a_j + 1)S(i,j), \quad i, j \in L(1,2), \quad i \neq j.$$

If we choose our notation so that

$$L(1,2) = \{1, 2, \dots, q+1\},$$

then we have

$$T(i,j) + (q-1)a_i a_j = (a_i + a_j + 1)S(i,j), \quad 1 \leq i < j \leq q+1 \quad (4.14)$$

We now proceed to solve the system of equations (4.14). Suppose $a_i \neq a_j$ for some $i \neq j$, $i, j \in L(1,2)$; in particular, say $a_1 \neq a_2$.

Case 1: $q \geq 3$.

We choose the equations

$$T(1,3) + (q-1)a_1 a_3 = (a_1 + a_3 + 1)S(1,3) \quad (4.15)$$

$$T(2,3) + (q-1)a_2 a_3 = (a_2 + a_3 + 1)S(2,3) \quad (4.16)$$

$$T(1,4) + (q-1)a_1 a_4 = (a_1 + a_4 + 1)S(1,4) \quad (4.17)$$

$$T(2,4) + (q-1)a_2 a_4 = (a_2 + a_4 + 1)S(2,4) \quad (4.18)$$

Subtracting (4.16) from (4.15), we get

$$a_2^2 - a_1^2 + (q-1)(a_1 - a_2)a_3 = (a_2 - a_1)a_3 + (a_2 - a_1) + (a_1 - a_2) \sum_{j=4}^{q+1} a_j$$

Since $a_1 \neq a_2$,

$$a_2 + a_1 - (q-1)a_3 = a_3 + 1 - \sum_{j=4}^{q+1} a_j$$

or

$$a_2 + a_1 = qa_3 + 1 - \sum_{j=4}^{q+1} a_j \quad (4.19)$$

Similarly, subtracting (4.18) from (4.17), we get

$$a_2 + a_1 = qa_4 + 1 - \sum_{\substack{j=3 \\ j \neq 4}}^{q+1} a_j \quad (4.20)$$

(4.19) and (4.20) give

$$q(a_3 - a_4) + (a_3 - a_4) = 0$$

$$\text{or} \quad (q+1)(a_3 - a_4) = 0$$

Since $q+1 \neq 0$ in K , we get $a_3 = a_4$.

There was nothing special about the choice of a_1, a_2, a_3 and a_4 , the same treatment yields that if $a_i \neq a_j$ for $i \neq j, i, j \in L(1, 2)$, then $a_k = a_1 \forall k, k \in L(1', 2')$. In particular, if $a_1 \neq a_2$, then $a_3 = a_4 = \dots = a_{q+1}$. Therefore the system (4.14) reduces to three equations, viz.,

$$T(1, 2) + (q-1)a_1a_2 = (a_1 + a_2 + 1)S(1, 2) \quad (4.21)$$

$$T(1, 3) + (q-1)a_1a_3 = (a_1 + a_3 + 1)S(1, 3) \quad (4.22)$$

$$T(2, 3) + (q-1)a_2a_3 = (a_2 + a_3 + 1)S(2, 3) \quad (4.23)$$

Case 2: $q = 2$.

In this case the system (4.14) consists exactly of the equations (4.21), (4.22) and (4.23) obtained in case 1.

Putting $a_j = d$ for $j \geq 3$ in (4.21), we get

$$(q-1)d^2 + (q-1)a_1a_2 = (a_1 + a_2 + 1)(q-1)d$$

Since $q-1 \neq 0$ in K ,

$$d^2 + a_1a_2 = (a_1 + a_2 + 1)d \quad (4.24)$$

Putting $a_j = d$ for $j \geq 3$ in (4.22), we get

$$a_2^2 + (q-2)d^2 + (q-1)a_1d = (a_1+d+1)(a_2+(q-2)d)$$

or
$$a_2^2 - a_1a_2 - a_2 = a_2d - a_1d + (q-2)d \quad (4.25)$$

Similarly, from (4.23), we get

$$a_1^2 - a_1a_2 - a_1 = a_1d - a_2d + (q-2)d \quad (4.26)$$

Subtracting (4.25) from (4.26),

$$a_1^2 - a_2^2 - a_1 + a_2 = 2(a_1 - a_2)d$$

Since $a_1 \neq a_2$, we get

$$a_1 + a_2 - 1 = 2d \quad (4.27)$$

Case 1: $\text{ch}(K) \neq 2$.

If $\text{ch}(K) \neq 2$, $d = \frac{a_1 + a_2 - 1}{2}$

Putting the value of d in (4.26) and simplifying, we get

$$a_1^2 + a_2^2 - 2a_1a_2 - (q-1)a_1 - (q-1)a_2 + (q-2) = 0 \quad (4.28)$$

Similarly, from (4.25), we get

$$a_1^2 + a_2^2 - 2a_1a_2 + 2a_1 + 2a_2 - 3 = 0 \quad (4.29)$$

Subtracting (4.29) from (4.28),

$$(q+1)a_1 + (q+1)a_2 - (q+1) = 0$$

Since $q+1 \neq 0$ in K , we get

$$a_1 + a_2 = 1$$

Hence $d = (a_1 + a_2 - 1)/2$ gives $d = 0$. Therefore from (4.24),

$a_1a_2 = 0$, that is, $a_1 = 0$ or $a_2 = 0$.

Case 2: $\text{ch}(K) = 2$.

If $\text{ch}(K) = 2$, it follows from (4.27) that

$$a_1 + a_2 = 1$$

Hence from (4.26), we get

$$a_1^2 - a_1(1-a_1) - a_1 = a_1d - (1-a_1)d + qd$$

$$\text{or } a_1^2 - a_1 + a_1^2 - a_1 = a_1d - d + a_1d + qd$$

$$\text{or } (q-1)d = 0$$

Since $q-1 \neq 0$ in K , $d = 0$. Therefore, once again from (4.24), we get $a_1a_2 = 0$, so $a_1 = 0$ or $a_2 = 0$.

Hence in any case we get that if two a_j 's are unequal, then one of them is zero, the other is one, and all other a_k 's on that line are zero.

Suppose all a_j 's on one line are equal, say, $a_1 = a_2 = \dots = a_{q+1} = d$. Then the system of equations (4.14) reduces to a single equation

$$(q-1)d^2 + (q-1)d^2 = (2d+1)(q-1)d$$

Since $q-1 \neq 0$ in K , we get $2d^2 = (2d+1)d$, or $d = 0$. So if all a_j 's on a line are equal, then all of them are zero.

If all a_j 's are equal, say $a_j = d \forall j$, $1 \leq j \leq n+1$, then $\sigma(x_1) = d(x_1 + x_2 + \dots + x_{n+1}) = 0$, a contradiction. Hence $\exists i, j$ such that $a_i \neq a_j$. Without loss of generality, let $a_i = 1$, $a_j = 0$. Hence $a_k = 0 \forall k \in L(i', j)$. But then if l lies on any line containing i , $l \neq i$, we get that

$a_1 = 0$. Since the union of all lines passing through i is Ω , it follows that $a_i = 1$, $a_j = 0 \forall j \in \Omega, j \neq i$. Therefore $\sigma(x_1) = x_1$, that is, $\sigma(x_1) \in \{x_1, x_2, \dots, x_{n+1}\}$. But this shows that $\text{Aut}(A)$ permutes $\{x_1, x_2, \dots, x_{n+1}\}$ and hence $\text{Aut}(A) \subseteq \Sigma_{n+1}$.

By corollary 3.3.4, $\text{Aut}(A) \cong \text{PFL}(m, q)$.

CHAPTER V
DETERMINATION OF THE AUTOMORPHISM GROUP
OF A IN THE CASE $b = a + c$, $b \neq 0$, $c \neq 0$

§1. THE ALGEBRA A

Since $b \neq 0$, without loss of generality we can assume that $b=1$. From $b=a+c$, we get $a=1-c$ and it follows from $a+(n-1)b=(q-1)c$ that $c=n/q$.

Throughout this chapter, we assume that $\text{ch}(K) > |a|$, where $a=1-n/q$ is considered as an integer. We also assume that $n+1 \neq 0$ in K . Since $|a|=c-1=q(q^{m-3}+\dots+q+1)$, and $m \geq 3$, as an integer $|a| > q$, so $q \neq 0$ in K . Hence $q^{m-1} \neq 0$ in K . But $q^{m-1}=n+a$, so $n+a \neq 0$ in K .

From equation (3.1) we get

$$\begin{aligned} x_i x_i &= (1-c)x_i, \quad 1 \leq i \leq n+1 \\ x_i x_j &= x_i + x_j + c \sum_{k \in L(i', j')} x_k, \quad 1 \leq i < j \leq n+1 \end{aligned}$$

For the remaining of this chapter, $\sum_i$ stands for $\sum_{i=1}^n$.
Let $\sum_i a_i x_i, \sum_i b_i x_i \in A$.

$$\begin{aligned} (\sum_i a_i x_i)(\sum_i b_i x_i) &= \sum_i a_i b_i x_i^2 + \sum_{i \neq j} a_i b_j x_i x_j \\ &= (1-c) \sum_i a_i b_i x_i + \sum_{i \neq j} a_i b_j (x_i + x_j + c \sum_{k \in L(i', j')} x_k) \end{aligned}$$

$$\begin{aligned}
&= \sum_i ((1-c)a_i b_i + \sum_{j \neq i} (a_i b_j + a_j b_i)) + c \left(\sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k \neq l}} a_k b_l \right) + \right. \\
&\quad \left. \sum_{\substack{k, l \in L(i', n+1') \\ k \neq l}} a_k b_l \right) x_i + c \left(\sum_{L \ni n+1} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k \neq l}} a_k b_l \right) \right) x_{n+1} \\
&= \sum_i ((1-c)a_i b_i + \sum_{j \neq i} (a_i b_j + a_j b_i)) + c \left(\sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k \neq l}} a_k b_l \right) + \right. \\
&\quad \left. \sum_{\substack{k, l \in L(i', n+1') \\ k \neq l}} a_k b_l - \sum_{L \ni n+1} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k \neq l}} a_k b_l \right) \right) x_i,
\end{aligned}$$

where L is any line.

Therefore

$$(\sum_i a_i x_i)(\sum_i b_i x_i) = \sum_i (-(1+c)a_i b_i + a_i S_b + b_i S_a + c(E_i - F)) x_i, \quad (5.1)$$

$$\text{where } S_a = \sum_i a_i, \quad S_b = \sum_i b_i,$$

$$E_i = \sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k \neq l}} a_k b_l \right) + \sum_{\substack{k, l \in L(i', n+1') \\ k \neq l}} a_k b_l,$$

$$\text{and } F = \sum_{L \ni n+1} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k \neq l}} a_k b_l \right).$$

§2. THE RELATION OBTAINED FROM THE MINIMAL
POLYNOMIAL

Putting $b=1$ in equation (3.2) we get that $\forall \sigma \in \text{Aut}(A)$,
 $\forall x \in A$, $\forall x_i$, $1 \leq i \leq n$,

$$\sigma(x_i)(\sigma(x_i)x) = (2+(q-2)c)\sigma(x_i)x + ((q-1)c^2 - (q-2)c - 1)x$$

Since $n = qc$, we get

$$\sigma(x_i)(\sigma(x_i)x) = (n-2c+2)\sigma(x_i)x + (c-1)(n-c+1)x \quad (5.2)$$

§3. CALCULATION OF THE AUTOMORPHISM GROUP OF A

We now proceed to show that $\text{Aut}(A)$ permutes the set
 $\{x_1, x_2, \dots, x_{n+1}\}$, that is, $\sigma(x_1) \in \{x_1, x_2, \dots, x_{n+1}\}$
 $\forall \sigma \in \text{Aut}(A)$.

$$\text{Let } \sigma(x_1) = a_1x_1 + a_2x_2 + \dots + a_nx_n.$$

$$\text{Since } x_1^2 = (1-c)x_1, \quad (x_1)^2 = (1-c)(x_1)$$

$$\text{or} \quad (\sum_i a_i x_i)^2 = (1-c) \sum_i a_i x_i$$

Putting $a_i = b_i$ in equation (5.1) we get

$$(\sum_i a_i x_i)^2 = \sum_i (-(1+c)a_i^2 + 2a_i S_a + 2c(\sum_{\substack{L \ni i \\ L \not\ni n+1}} (\sum_{\substack{k, l \in L \setminus \{i\} \\ k < l}} a_k a_l)) +$$

$$\sum_{\substack{k, l \in L(i', n+1') \\ k < l}} a_k a_l - P_{n+1}))x_i,$$

$$\text{where } P_{n+1} = \sum_{L \ni n+1} (\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k < l}} a_k a_l).$$

Hence for $1 \leq i \leq n$,

$$\begin{aligned}
 & -(1+c)a_i^2 + 2a_i S_a + 2c \left(\sum_{\substack{L \ni i \\ L \neq n+1}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k < l}} a_k a_l \right) \right) + \\
 & \quad \sum_{\substack{k, l \in L(i', n+1') \\ k < l}} a_k a_l - P_{n+1} = (1-c)a_i \quad (5.3)
 \end{aligned}$$

Summing equations (5.3) from $i=1$ to $i=n$, we get

$$\begin{aligned}
 & -(1+c) \sum_i a_i^2 + 2S_a^2 + 2(q-1)c \sum_i \left(\sum_{\substack{k, l \in L(i', n+1') \\ k < l}} a_k a_l \right) + \\
 & \quad 2(q-2)cP_{n+1} - 2ncP_{n+1} = (1-c)S_a \\
 \text{or } & -(1+c) \sum_i a_i^2 + 2S_a^2 - (q-1)c \sum_i a_i^2 + (q-1)c \sum_i a_i^2 + \\
 & 2(q-1)c \sum_{i < j} a_i a_j - 2(q-1)cP_{n+1} + 2(q-2)cP_{n+1} - 2ncP_{n+1} = \\
 & \quad (1-c)S_a \\
 \text{or } & (n+1)T - (n-c+2)S_a^2 + 2(n+1)cP_{n+1} + (1-c)S_a = 0 \quad (5.4)
 \end{aligned}$$

where $T = \sum_i a_i^2$.

We now put $i=1$ and $x=x_r$ in equation (5.2) to get

$$\sigma(x_1)(\sigma(x_1)x_r) = (n-2c+2)\sigma(x_1)x_r + (c-1)(n-c+1)x_r \quad (5.5)$$

for $1 \leq r \leq n$.

$$\text{Let } \sigma(x_i)x_r = \sum_i b_i(r)x_i, \quad 1 \leq r \leq n.$$

(Notice that $b_i(r)$ here is different from $b_i(r)$ used in chapter IV).

Using equation (5.1) $b_r=1$, $b_j=0$ if $j \neq r$, we get

$$b_i(r) = \begin{cases} S_a - c \sum_{i \in L(r, n+1')} a_i, & \text{if } i = r \\ a_i + c \left(\sum_{k \in L(i', r')} a_k - \sum_{k \in L(r', n+1')} a_k \right), & \text{if } i \notin L(r, n+1) \\ (1-c)a_i, & \text{if } i \in L(r', n+1') \end{cases}$$

—— (5.6)

$$\text{Let } \sigma(x_1)(\sigma(x_1)x_r) = \sum_i d_i(r)x_i, \quad 1 \leq r \leq n.$$

From equation (5.1) we get that for $1 \leq r \leq n$, $1 \leq i \leq n$,

$$d_i(r) = -(1+c)a_i b_i(r) + a_i S_b(r) + b_i(r) S_a + c(E_i(r) - F(r))$$

—— (5.7)

$$\text{where } S_b(r) = \sum_i b_i(r), \quad F(r) = \sum_{L \ni n+1} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k \neq l}} a_k b_l(r) \right),$$

$$\text{and } E_i(r) = \sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k \neq l}} a_k b_l(r) \right) + \sum_{\substack{k, l \in L(i', n+1') \\ k \neq l}} a_k b_l(r).$$

From (5.5) we get

$$d_r(r) = (n-2c+2)b_r(r) + (c-1)(n-c+1) \quad (5.8)$$

$$\text{and for } i \neq r, \quad d_i(r) = (n-2c+2)b_i(r) \quad (5.9)$$

Lemma 5.3.1: For $1 \leq r \leq n$,

$$S_b(r) = (n-c+2)S_a - (n+1)a_r - (n+1)c \sum_{i \in L(r', n+1')} a_i.$$

$$\text{Proof: } S_b(r) = \sum_i b_i(r) = b_r(r) + \sum_{i \notin L(r, n+1)} b_i(r) + \sum_{i \in L(r', n+1')} b_i(r)$$

Using equation (5.6),

$$\begin{aligned} S_b(r) &= S_a - c \sum_{i \in L(r, n+1')} a_i + \sum_{i \notin L(r, n+1)} a_i + c(q-1) \sum_{i \notin L(r, n+1)} a_i \\ &\quad - c(n-q) \sum_{i \in L(r', n+1')} a_i + (1-c) \sum_{i \in L(r', n+1')} a_i \\ &= S_a - ca_r - c \sum_{i \in L(r', n+1')} a_i + (c(q-1)+1) \sum_{i \notin L(r, n+1)} a_i + \\ &\quad (c(q-1)+1)a_r - (c(q-1)+1)a_r + (c(q-1)+1) \sum_{i \in L(r', n+1')} a_i - \\ &\quad (c(q-1)+1) \sum_{i \in L(r', n+1')} a_i - c(n-q) \sum_{i \in L(r', n+1')} a_i + \\ &\quad (1-c) \sum_{i \in L(r', n+1')} a_i \\ &= (n-c+2)S_a - (n+1)a_r - (n+1)c \sum_{i \in L(r', n+1')} a_i \end{aligned}$$

Lemma 5.3.2: $\sum_i b_i(i) = 0$.

Proof: From equation (5.6),

$$\sum_i b_i(i) = nS_a - c \sum_i \left(\sum_{j \in L(i, n+1')} a_j \right)$$

$$= nS_a - qcS_a = nS_a - nS_a = 0, \text{ since each line containing } n+1 \text{ has } q \text{ other points.}$$

Lemma 5.3.3: $\sum_i a_i b_i(i) = S_a^2 - cT - 2cP_{n+1}.$

Proof: From equation (5.6),

$$\begin{aligned}
 \sum_i a_i b_i(i) &= \sum_i a_i (S_a - c \sum_{j \in L(i, n+1')} a_j) \\
 &= S_a \sum_i a_i - c \sum_i a_i \left(\sum_{j \in L(i, n+1')} a_j \right) \\
 &= S_a^2 - c \sum_i a_i^2 - 2c \sum_{\substack{L \ni n+1 \\ k, l \in L \setminus \{n+1\} \\ k < l}} (a_k a_l) \\
 &= S_a^2 - cT - 2cP_{n+1}.
 \end{aligned}$$

Lemma 5.3.4: $\sum_i a_i S_b(i) = (n-c+2)S_a^2 - (n+1)T - 2(n+1)cP_{n+1}.$

Proof: From lemma 5.3.1,

$$\begin{aligned}
 \sum_i a_i S_b(i) &= \sum_i a_i ((n-c+2)S_a - (n+1)a_i - (n+1)c \sum_{j \in L(i', n+1')} a_j) \\
 &= (n-c+2)S_a^2 - (n+1)T - (n+1)c \sum_i a_i \left(\sum_{j \in L(i', n+1')} a_j \right) \\
 &= (n-c+2)S_a^2 - (n+1)T + 2(n+1)cP_{n+1}.
 \end{aligned}$$

Lemma 5.3.5: For $1 \leq j \leq n$, $\sum_i b_j(i) = S_a - a_j - c \sum_{k \in L(j', n+1')} a_k.$

Proof:

$$\sum_i b_j(i) = b_j(j) + \sum_{i \notin L(j, n+1)} b_j(i) + \sum_{i \in L(j', n+1')} b_j(i)$$

$$\begin{aligned}
&= S_a - c \sum_{i \in L(j, n+1)'} a_i + \sum_{i \notin L(j, n+1)} (a_j + c(\sum_{k \in L(i', j')} a_k - \sum_{k \in L(i', n+1)'} a_k)) + (1-c)(q-1)a_j \\
&= S_a - ca_j - c \sum_{i \in L(j', n+1)'} a_i + (n-q)a_j + \\
&\quad (q-1)c \sum_{k \notin L(j, n+1)} a_j - (q-1)c \sum_{k \notin L(j', n+1)} a_j + (1-c)(q-1)a_j \\
&= S_a - a_j - c \sum_{k \in L(j', n+1)'} a_k .
\end{aligned}$$

Lemma 5.3.6:

$$\sum_i F(i) = (q-1)S_a^2 - (q-1)cT - 2(n+1-2c)P_{n+1}$$

Proof:

$$\begin{aligned}
\sum_i F(i) &= \sum_i \left(\sum_{l \in L(n+1)} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k \neq l}} a_k b_l(i) \right) \right) \\
&= \sum_{l \in L(n+1)} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k \neq l}} a_k \left(\sum_i b_l(i) \right) \right) \\
&= \sum_{l \in L(n+1)} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k \neq l}} a_k (S_a - a_l - c \sum_{r \in L(l', n+1)'} a_r) \right) \\
&= (q-1)S_a \sum_i a_i - 2 \sum_{l \in L(n+1)} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k < l}} a_k a_l \right) + (q-1)c \sum_i a_i^2 \\
&\quad - 2(q-2)c \sum_{l \in L(n+1)} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k < l}} a_k a_l \right) \\
&= (q-1)S_a^2 - (q-1)cT - 2(n+1-2c)P_{n+1}.
\end{aligned}$$

Lemma 5.3.7: For a fixed i ,

$$\sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, 1 \leq k \leq L \setminus \{i\} \\ k \neq 1}} b_k(1) \right) = (q-1)(1-c)(S_a - \sum_{j \in L(i', n+1')} a_j - (n+1)a_i)$$

Proof:

$$\begin{aligned} \sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, 1 \leq k \leq L \setminus \{i\} \\ k \neq 1}} b_k(1) \right) &= (q-1) \sum_{j \in L(i, n+1)} a_j + (n-q)(q-1)ca_i + \\ &\quad c(q-2)(q-1) \sum_{j \in L(i, n+1)} a_j - c(q-1)^2 \sum_{j \in L(i, n+1)} a_j \\ &= (n-q)(q-1)ca_i + (q-1)(1-c) \sum_{j \in L(i, n+1)} a_j \\ &= (q-1)((n-q)ca_i + (1-c)S_a - \\ &\quad (1-c) \sum_{j \in L(i', n+1')} a_j - (1-c)a_i) \\ &= (q-1)((1-c)S_a - (1-c) \sum_{j \in L(i', n+1')} a_j + \\ &\quad (nc-n-1+c)a_i) \\ &= (q-1)(1-c)(S_a - \sum_{j \in L(i', n+1')} a_j - (n+1)a_i) \end{aligned}$$

Lemma 5.3.8: For a fixed i ,

$$\sum_{\substack{k, 1 \leq k \leq L(i', n+1') \\ k \neq 1}} b_k(1) = (1-c)(q-2) \sum_{j \in L(i', n+1')} a_j$$

Proof: This trivially follows from equation (5.6).

Lemma 5.3.9:

$$\sum_i E_i(i) = (1-c)((q-1)S_a^2 - (q-1)(n+1)T - P_{n+1})$$

Proof:

$$\begin{aligned} \sum_i E_i(i) &= \sum_i \left(\sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k \neq l}} a_k b_l(i) \right) + \sum_{\substack{k, l \in L(i', n+1') \\ k \neq l}} a_k b_l(i) \right) \\ &= \sum_i a_i \left(\sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k \neq l}} b_k(1) \right) + \sum_{\substack{k, l \in L(i', n+1') \\ k \neq l}} b_k(1) \right) \\ &= \sum_i a_i \left((1-c)(q-1)(S_a - (n+1)a_i - \sum_{j \in L(i', n+1')} a_j) \right. \\ &\quad \left. + (1-c)(q-2) \sum_{j \in L(i', n+1')} a_j \right) \\ &= \sum_i a_i \left((1-c)(q-1)S_a - (1-c)(q-1)(n+1)a_i \right. \\ &\quad \left. - (1-c) \sum_{j \in L(i', n+1')} a_j \right) \\ &= (1-c)((q-1)S_a^2 - (q-1)(n+1)T - 2P_{n+1}) \end{aligned}$$

We now put $i=r$ in equation (5.7) and sum from $r=1$ to $r=n$ to get

$$\begin{aligned} \sum_r d_r(r) &= -(1+c) \sum_r a_r b_r(r) + \sum_r a_r S_b(r) + c(\sum_r E_r(r) - \sum_r F(r)) \\ &\quad + S_a \sum_r b_r(r) \end{aligned}$$

Using lemmas 5.3.3, 5.3.4, 5.3.6 and 5.3.9, it follows

that

$$\begin{aligned}
\sum_r d_r(r) &= -(1+c)(S_a^2 - cT - 2cP_{n+1}) + (n-c+2)S_a^2 - (n+1)T \\
&\quad - 2(n+1)cP_{n+1} + c((1-c)((q-1)S_a^2 - (q-1)(n+1)T \\
&\quad - 2P_{n+1}) - ((q-1)S_a^2 - (q-1)cT - 2(n+1-2c)P_{n+1})) \\
&= (1+c)S_a^2 + c(1+c)T + 2c(1+c)P_{n+1} + (n-c+2)S_a^2 \\
&\quad - (n+1)T - 2(n+1)cP_{n+1} + c(-c(q-1)S_a^2 + \\
&\quad (q-1)(2c-n+nc-1)T + 2(n-c)P_{n+1}) \\
&= (-1-c+n-c+2-c^2(q-1))S_a^2 + (c(1+c) - (n+1) + \\
&\quad (n-c)(2c-n+nc-1))T + (2c(1+c) - 2(n+1)c + \\
&\quad 2c(n-c))P_{n+1} \\
&= (1-2c+n-nc+c^2)S_a^2 + (n^2+c^2+nc^2-n^2c-3nc+2n-2c+1)T
\end{aligned}$$

$$\text{Hence } \sum_r d_r(r) = (1-c)(n-c+1)S_a^2 - (n+1)(1-c)(n-c+1)T$$

Summing equation (5.8) from $r=1$ to $r=n$, we get

$$\sum_r d_r(r) = (n-2c+2)\sum_r b_r(r) + n(c-1)(n-c+1)$$

Therefore from lemma 5.3.2

$$\sum_r d_r(r) = n(c-1)(n-c+1)$$

Comparing the two values of $\sum_r d_r(r)$, we get

$$(1-c)(n-c+1)S_a^2 - (n+1)(1-c)(n-c+1)T = n(c-1)(n-c+1)$$

But $n-c+1 = n+a \neq 0$ in K , and $1-c \neq 0$ in K since

$\text{ch}(K) > |a| = c-1$. Therefore we get

$$S_a^2 - (n+1)T = -n \quad (5.10)$$

We now consider equation (5.9), viz.,

$$d_i(r) = (n-2c+2)b_i(r), \quad i \neq r$$

We fix an i , and sum over r such that $r \notin L(i, n+1)$ to get

$$\sum_{r \notin L(i, n+1)} d_i(r) = (n-2c+2) \sum_{r \notin L(i, n+1)} b_i(r) \quad (5.11)$$

From equation (5.7),

$$\begin{aligned} \sum_{r \notin L(i, n+1)} d_i(r) &= -(1+c) \sum_{r \notin L(i, n+1)} a_i b_i(r) + a_i \sum_{r \notin L(i, n+1)} S_b(r) \\ &\quad + S_a \sum_{r \notin L(i, n+1)} b_i(r) + c \sum_{r \notin L(i, n+1)} (E_i(r) - F(r)) \end{aligned} \quad (5.12)$$

Lemma 5.3.10: If $j \notin L(i, n+1')$, then

$$\sum_{k \notin L(i, n+1)} b_j(k) = (n-q)a_j$$

Proof: From equation (5.6),

$$\begin{aligned} \sum_{k \notin L(i, n+1)} b_j(k) &= \sum_{k \notin L(i, n+1)} (a_j + c(\sum_{l \in L(j', k')} a_l - \sum_{l \in L(k', n+1')} a_l)) \\ &= (n-q)a_j + c(\sum_{k \notin L(i, n+1)} (\sum_{l \in L(j', k')} a_l) \\ &\quad - \sum_{k \notin L(i, n+1)} (\sum_{l \in L(k', n+1')} a_l)) \\ &= (n-q)a_j + c((q-1) \sum_{k \notin L(i, n+1)} a_k - (q-1) \sum_{k \notin L(i, n+1)} a_k) \\ &= (n-q)a_j \end{aligned}$$

Lemma 5.3.11: If $j \notin L(i, n+1)$, then

$$\begin{aligned} \sum_{k \notin L(i, n+1)} b_j(k) &= S_a - (q+1)a_j - c \sum_{k \in L(j', n+1')} a_k + \\ &\quad c(q-1) \sum_{k \in L(i', n+1')} a_k - c \sum_{l \in L(j, n+1')} \left(\sum_{k \in L(i', 1')} a_k \right) \end{aligned}$$

Proof:

$$\begin{aligned} \sum_{k \notin L(i, n+1)} b_j(k) &= b_j(j) + \sum_{k \in L(j', n+1')} b_j(k) + \sum_{k \notin L(i, n+1) \cup L(j, n+1)} b_j(k) \\ &= S - c \sum_{k \in L(j, n+1')} a_k + (1-c)(q-1)a_j + \\ &\quad \sum_{k \notin L(i, n+1) \cup L(j, n+1)} a_j + c \sum_{l \in L(j', k')} a_l - c \sum_{l \in L(k', n+1')} a_l \\ &= S_a - c \sum_{k \in L(j, n+1')} a_k + (1-c)(q-1)a_j + (q-1)S_a - \\ &\quad \sum_{k \in L(j, n+1')} \left(\sum_{l \in L(i', k')} a_l \right) - (q-1) \sum_{k \in L(j, n+1')} a_k - \\ &\quad (q-1)S_a + (q-1) \left(\sum_{k \in L(i, n+1')} a_k + \sum_{k \in L(j, n+1')} a_k \right) \\ &= S_a - c \sum_{k \in L(j, n+1')} a_k + (1-c)(q-1)a_j + (n-2q)a_j + \\ &\quad c((q-1) \sum_{k \in L(i, n+1')} a_k - \sum_{k \in L(j, n+1')} a_k) \\ &= S_a - (q+1)a_j - c \sum_{k \in L(j', n+1')} a_k + \\ &\quad c(q-1) \sum_{k \in L(i, n+1')} a_k - c \sum_{l \in L(j, n+1')} \left(\sum_{k \in L(i', 1')} a_k \right) \end{aligned}$$

Lemma 5.3.12:

$$\sum_{j \notin L(i, n+1)} S_b(j) = (n-nq-2q+c-1)S_a + (n+1)(n+1-c) \sum_{j \in L(i, n+1')} a_j$$

Proof:

$$\begin{aligned} \sum_{j \notin L(i, n+1)} S_b(j) &= \sum_{j \notin L(i, n+1)} ((n-c+2)S_a - (n+1)a_j - (n+1)c \sum_{k \in L(j', n+1')} a_k) \\ &= (n-c+2)(n-q)S_a - (n+1) \sum_{j \notin L(i, n+1)} a_j - \\ &\quad (n+1)c \sum_{j \notin L(i, n+1)} \left(\sum_{k \in L(j', n+1')} a_k \right) \\ &= (n-c+2)(n-q)S_a - (n+1) \sum_{j \notin L(i, n+1)} a_j - \\ &\quad (n+1)c(q-1) \sum_{j \notin L(i, n+1)} a_k \\ &= (n-c+2)(n-q)S_a - ((n+1) + (n+1)c(q-1)) \times \\ &\quad (S_a - \sum_{j \in L(i, n+1')} a_j) \\ &= (n-nq-2q+c-1)S_a + (n+1)(n+1-c) \sum_{j \in L(i, n+1')} a_j \end{aligned}$$

Lemma 5.3.13:

$$\sum_{k \notin L(i, n+1)} \left(\sum_{l \in L(k', n+1')} a_l \right) = 2(P_{n+1} - \sum_{\substack{k, l \in L(i, n+1') \\ k < l}} a_k a_l)$$

Proof: It follows from a trivial rearrangement of terms.

Lemma 5.3.14: For $1 \leq i, j \leq n$,

$$E_i(j) - F(j) = -a_i \sum_{k \in L(i', n+1')} b_k(j) - b_i(j) \sum_{k \in L(i', n+1')} a_k + \\ \sum_{k \notin L(i, n+1)} a_k \left(\sum_{l \in L(i', k')} b_l(j) - \sum_{l \in L(k', n+1')} b_l(j) \right)$$

Proof: This follows from the definition of $E_i(j)$ and $F(j)$, and a rearrangement of terms.

Lemma 5.3.15: For any fixed k, i with $k \notin L(i, n+1)$,

$$\sum_{j \notin L(i, n+1)} \left(\sum_{l \in L(i', k')} b_l(j) - \sum_{l \in L(k', n+1')} b_l(j) \right) = \\ - (q+1-c) \left(\sum_{l \in L(i', k')} a_l - \sum_{l \in L(k', n+1')} a_l \right)$$

Proof: This follows from lemma 5.3.11 and rearrangement of terms.

From equations (5.11) and (5.12) we get that for a fixed i , $1 \leq i \leq n$,

$$- (1+c) \sum_{r \notin L(i, n+1)} a_i b_i(r) + a_i \sum_{r \notin L(i, n+1)} S_b(r) + S_a \sum_{r \notin L(i, n+1)} b_i(r) + \\ c \sum_{r \notin L(i, n+1)} (E_i(r) - F(r)) = (n-2c+2) \sum_{r \notin L(i, n+1)} b_i(r)$$

From lemma 5.3.14 we get that

$$\begin{aligned}
& - (1+c)a_i \sum_{r \notin L(i, n+1)} b_i(r) + a_i \sum_{r \notin L(i, n+1)} S_b(r) + S_a \sum_{r \notin L(i, n+1)} b_i(r) \\
& + c \sum_{r \notin L(i, n+1)} (-a_i \sum_{k \in L(i', n+1')} b_k(r) - b_i(r) \sum_{k \in L(i', n+1')} a_k) \\
& + \sum_{k \notin L(i, n+1)} a_k (\sum_{l \in L(i', k')} b_l(r) - \sum_{l \in L(k', n+1')} b_l(r)) = (n-2c+2) \sum_{r \notin L(i, n+1)} b_i(r) \\
\text{or } & - (1+c)a_i \sum_{r \notin L(i, n+1)} b_i(r) + a_i \sum_{r \notin L(i, n+1)} S_b(r) + S_a \sum_{r \notin L(i, n+1)} b_i(r) \\
& - ca_i \sum_{k \in L(i', n+1')} (\sum_{r \notin L(i, n+1)} b_k(r)) - c (\sum_{k \in L(i', n+1')} a_k) (\sum_{r \notin L(i, n+1)} b_i(r)) \\
& + c \sum_{k \notin L(i, n+1)} (\sum_{r \notin L(i, n+1)} a_k (\sum_{l \in L(i', k')} b_l(r) - \sum_{l \in L(k', n+1')} b_l(r))) \\
& = (n-2c+2) \sum_{r \notin L(i, n+1)} b_i(r)
\end{aligned}$$

By lemmas 5.3.10 and 5.3.12,

$$\begin{aligned}
& - (1+c)a_i(n-q)a_i + a_i((n-nq-2q+c-1)S_a \\
& + (n+1)(n+1-c) \sum_{j \in L(i, n+1')} a_j) + S_a(n-q)a_i - ca_i \sum_{k \in L(i', n+1')} (n-q)a_k \\
& - c(n-q)a_i \sum_{k \in L(i', n+1')} a_k + c \sum_{k \notin L(i, n+1)} (-(q+1-c)a_k (\sum_{l \in L(i', k')} a_l \\
& - \sum_{l \in L(k', n+1')} a_l)) = (n-2c+2)(n-q)a_i
\end{aligned}$$

$$\begin{aligned}
& \text{or} \quad - (1+c)(n-q)a_i^2 + (n-nq-2q+c-1)a_i S_a + (n+1)(n+1-c)a_i^2 \\
& + (n+1)(n+1-c)a_i \sum_{j \in L(i', n+1')} a_j + (n-q)a_i S_a \\
& - 2c(n-q)a_i \sum_{k \in L(i', n+1')} a_k - c(q+1-c) \sum_{k \notin L(i, n+1)} a_k \left(\sum_{l \in L(i', k')} a_l \right. \\
& \left. - \sum_{l \in L(k', n+1')} a_l \right) = (n-c+2)(n-q)a_i \\
& \text{or} \quad (n^2-2nc+2n-c+q+1)a_i^2 + (2n-nq+c-3q-1)a_i S_a \\
& - c(q+1-c) \sum_{k \notin L(i, n+1)} a_k \left(\sum_{l \in L(i', k')} a_l - \sum_{l \in L(k', n+1')} a_l \right) \\
& + (n^2-3nc+4n-c+1)a_i \sum_{k \in L(i', n+1')} a_k = (n-2c+2)(n-q)a_i \\
& \text{or} \quad (n^2-2nc+2n-c+q+1)a_i^2 + (n^2-3nc+4n-c+1)a_i \sum_{k \in L(i', n+1')} a_k \\
& + (2n-nq+c-3q-1)a_i S_a + c(q+1-c) \left(2P_{n+1} - 2 \sum_{\substack{k, l \in L(i, n+1') \\ k < l}} a_k a_l \right) \\
& - c(q+1-c) \sum_{k \notin L(i, n+1)} a_k \left(\sum_{l \in L(i', k')} a_l \right) = (n-2c+2)(n-q)a_i \\
& \text{or} \quad (n^2-2nc+2n-c+q+1)a_i^2 + (n^2-3nc+4n-c+1)a_i \sum_{k \in L(i', n+1')} a_k \\
& + (2n-nq+c-3q-1)a_i S_a - 2c(q+1-c)a_i \sum_{k \in L(i', n+1')} a_k \\
& - 2c(q+1-c) \sum_{\substack{k, l \in L(i', n+1') \\ k < l}} a_k a_l - c(q+1-c) \sum_{k \notin L(i, n+1)} a_k \left(\sum_{l \in L(i', k')} a_l \right) \\
& + 2c(q+1-c)P_{n+1} = (n-2c+2)(n-q)a_i
\end{aligned}$$

$$\begin{aligned}
& \text{or } (n^2 - 2nc + 2n - c + q + 1)a_i^2 + (2n - nq + c - 3q - 1)a_i S_a \\
& + (n^2 + 2n - 3nc + 2c^2 - 3c + 1)a_i \sum_{k \in L(i', n+1')} a_k + 2c(q+1-c)P_{n+1} \\
& - 2c(q+1-c) \sum_{\substack{k, l \in L(i', n+1') \\ k < l}} a_k a_l - c(q+1-c) \sum_{k \notin L(i, n+1)} a_k \left(\sum_{l \in L(i', k')} a_l \right) \\
& = (n - 2c + 2)(n - q)a_i \quad (5.13)
\end{aligned}$$

We next list three results without proof, since all the three are consequences of easy rearrangements of terms.

Lemma 5.3.16:

$$\sum_j \left(\sum_{k \notin L(j, n+1)} a_k \left(\sum_{l \in L(j', k')} a_l \right) \right) = (q-1)(S_a^2 - T - 2P_{n+1})$$

Lemma 5.3.17: $\sum_j a_j \left(\sum_{k \in L(j', n+1')} a_k \right) = 2P_{n+1}$

Lemma 5.3.18: $\sum_j \left(\sum_{\substack{k, l \in L(j', n+1') \\ k < l}} a_k a_l \right) = (q-2)P_{n+1}$

We now sum the equation (5.13) from $i=1$ to $i=n$ to get

$$\begin{aligned}
& (n^2 - 2nc + 2n - c + q + 1)T + (2n - nq + c - 3q - 1)S_a^2 + \\
& + (n^2 + 2n - 3nc + 2c^2 - 3c + 1) \sum_i a_i \left(\sum_{k \in L(i', n+1')} a_k \right) \\
& - 2c(q+1-c) \sum_i \left(\sum_{\substack{k, l \in L(i', n+1') \\ k < l}} a_k a_l \right) + 2nc(q+1-c)P_{n+1} \\
& - c(q+1-c) \sum_i \left(\sum_{k \notin L(i, n+1)} a_k \left(\sum_{l \in L(i', k')} a_l \right) \right) = (n - 2c + 2)(n - q)S_a
\end{aligned}$$

Using lemmas 5.3.16, 5.3.17 and 5.3.18, we get

$$\begin{aligned}
 & (n^2 - 2nc + 2n - c + q + 1)T + (2n - nq + c - 3q - 1)S_a^2 + 2nc(q + 1 - c)P_{n+1} \\
 & + 2(n^2 + 2n - 3nc + 2c^2 - 3c + 1)P_{n+1} - 2c(q + 1 - c)(q - 2)P_{n+1} \\
 & - c(q + 1 - c)(q - 1)(S_a^2 - T - 2P_{n+1}) = (n - 2c + 2)(n - q)S_a \\
 \text{or } & (n^2 - 3nc + 2n + nq + c^2 - 2c + q + 1)T + (2n + nc - 2nq - 3q - c^2 + 2c - 1)S_a^2 \\
 & + 2(2n^2 + 3n - 2nc - nc^2 + c^2 - 2c + 1)P_{n+1} = (n^2 + 4n - 2nc - nq - 2q)S_a
 \end{aligned}$$

Multiplying by c , we get

$$\begin{aligned}
 & (n^2c - 3nc^2 + 2nc + n^2 + c^3 - 2c^2 + n + c)T + (2nc + nc^2 - 2n^2 - 3n - c^3 + 2c^2 - c)S_a^2 \\
 & + 2c(2n^2 + 3n - 2nc - nc^2 + c^2 - 2c + 1)P_{n+1} = (n^2c + 4nc - 2nc^2 - n^2 - 2n)S_a^2
 \end{aligned}$$

(5.14)

We now consider equations (5.4) and (5.10) along with (5.14), viz.,

$$(n+1)T - (n-c+2)S_a^2 + 2(n+1)cP_{n+1} = (c-1)S_a \quad (5.4)$$

$$(n+1)T - S_a^2 = n \quad (5.10)$$

Subtracting (5.10) from (5.4), we get

$$(n+1-c)S_a^2 - 2c(n+1)P_{n+1} = (1-c)S_a + n \quad (5.15)$$

Since $n+1 \neq 0$ in K , (5.10) yields

$$T = \frac{S_a^2 + n}{n+1}$$

Putting this value of T in (5.14), we get

$$\begin{aligned}
& (S_a^2 + n)(n^2c - 3nc^2 + 2nc + n^2 + c^3 - 2c^2 + n + c) \\
& + (n+1)(2nc + nc^2 - 2n^2 - 3n - c^3 + 2c^2 - c)S_a^2 \\
& + 2c(n+1)(2n^2 + 3n - 2nc - nc^2 + c^2 - 2c + 1)P_{n+1} \\
& = (n+1)(n^2c + 4nc - 2nc^2 - n^2 - 2n)S_a \\
\text{or} \quad & n(3nc + 3c - 4n - 2 + nc^2 - 2n^2 - c^3)S_a^2 \\
& + 2c(n+1)(2n^2 + 3n - 2nc - nc^2 - 2c + c^2 + 1)P_{n+1} \\
& = -n(n^2c + 2nc - 3nc^2 + n^2 + n - 2c^2 + c^3 + c) \\
& + n(n+1)(nc + 4c - 2c^2 - n - 2)S_a \tag{5.16}
\end{aligned}$$

Multiplying (5.15) by $(2n^2 + 3n - 2nc - nc^2 - 2c + c^2 + 1)$, and adding to (5.16), we get

$$\begin{aligned}
& (-n^2c - 4nc + n^2 + 2n - 3c + 3c^2 - c^3 + 2nc^2 + 1)S_a^2 \\
& = (-n^3 + nc^3 - c^3 + n^3c - 2n^2c^2 + 3n^2c - nc^2 - n^2 + 3c^2 - nc + n - 3c + 1)S_a \\
& + n(n^2 + 2n - 4nc + 2nc^2 - 3c + 3c^2 - n^2c - c^3 + 1)
\end{aligned}$$

Factoring the above expressions, we get

$$(1-c)(n-c+1)^2S_a^2 = (1-c)(1-n)(n-c+1)^2S_a + n(1-c)(n-c+1)^2$$

Since $1-c=a \neq 0$ in K , $n-c+1=n+a \neq 0$ in K , we get

$$S_a^2 = (1-n)S_a + n$$

$$\text{or} \quad S_a^2 + (n-1)S_a - n = 0 \quad (5.17)$$

or $(S_a+n)(S_a-1) = 0$. Hence $S_a = -n$ or $S_a = 1$. From (5.10) we get that if $S_a = 1$ then $T = 1$ and if $S_a = -n$ then $T = n$. Similarly, from (5.15) it follows that if $S_a = 1$ then $P_{n+1} = 0$ and if $S_a = -n$ then $P_{n+1} = n(n-c)/2c$

Therefore one of the following holds:

$$(i) \quad S_a = 1, T = 1, P_{n+1} = 0, \text{ or} \quad (5.18)$$

$$(ii) \quad S_a = -n, T = n, P_{n+1} = \frac{n(n-c)}{2c} = \frac{n(q-1)}{2}$$

We now proceed to calculate the a_i 's. From equation (5.3) we get that for $1 \leq i \leq n$,

$$\begin{aligned} 2c \sum_{\substack{L_1 \ni i \\ L_{n+1} \ni i}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k < l}} a_k a_l \right) &= (1+c)a_i^2 + (1-c-2S_a)a_i + 2cP_{n+1} \\ &\quad - 2c \sum_{\substack{k, l \in L(i', n+1') \\ k < l}} a_k a_l \end{aligned} \quad (5.19)$$

We fix a line L_1 containing $n+1$, and by renumbering if necessary, we can put $L_1 = \{1, 2, \dots, q, n+1\}$. Let $L_1' = \{1, 2, \dots, q\}$, and $L_1'' = \{2, 3, \dots, q\}$. From equations (5.7) and (5.8) we get

$$\begin{aligned} d_1(1) &= -(1+c)a_1 b_1(1) + a_1 S_b(1) + b_1(1) S_a + c(E_1(1) - F(1)) \\ &= (n-2c+2)b_1(1) + (c-1)(n-c+1) \end{aligned}$$

$$\begin{aligned} \text{or } & (1-c)(n-c+1) - (n-2c+2-S_a)b_1(1) - (1+c)a_1b_1(1) \\ & + a_1S_b(1) + c(E_1(1)-F(1)) = 0 \end{aligned} \quad (5.20)$$

From lemma (5.1)

$$\begin{aligned} S_b(1) &= (n-c+2)S_a - (n+1)a_1 - (n+1)c \sum_{i \in L_1''} a_i \\ &= (n-c+2)S_a - (n+1)a_1 - (n+1)cS_1 \end{aligned}$$

$$\text{where } S_1 = \sum_{i \in L_1''} a_i$$

From equation (5.6),

$$b_1(1) = S_a - c \sum_{i \in L_1'} a_i = S_a - ca_1 - cS_1$$

Putting these values of $S_b(1)$ and $b_1(1)$ in equation (5.20), we get

$$\begin{aligned} & (1-c)(n-c+1) - (n-2c+2-S_a)(S_a-ca_1-cS_1) \\ & - (1+c)a_1(S_a-ca_1-cS_1) + a_1((n-c+2)S_a-(n+1)a_1-(n+1)cS_1) \\ & + c(E_1(1) - F(1)) = 0 \end{aligned} \quad (5.21)$$

$$\begin{aligned} E_1(1) &= \sum_{\substack{L_1' \\ L_1' \neq \{1\}}} \left(\sum_{\substack{k, l \in L \setminus \{1\} \\ k \neq l}} a_k b_l(1) \right) + \sum_{\substack{k, l \in L_1'' \\ k \neq l}} a_k b_l(1) \\ &= \sum_{i \in L_1'} a_i \left(\sum_{j \in L(1', i')} b_j(1) \right) + \sum_{i \in L_1''} a_i \left(\sum_{j \in L_1'' \setminus \{i\}} b_j(1) \right) \end{aligned}$$

$$\begin{aligned}
F(1) &= \sum_{L \ni n+1} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k \neq l}} a_k b_l(1) \right) = \sum_i a_i \left(\sum_{j \in L(i', n+1')} b_j(1) \right) \\
&= \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', n+1')} b_j(1) \right) + a_1 \sum_{j \in L_1} b_j(1) + b_1(1) S_1 \\
&\quad + \sum_{i \in L_1} a_i \left(\sum_{j \in L_1 \setminus \{i\}} b_j(1) \right)
\end{aligned}$$

Therefore

$$\begin{aligned}
E_1(1) - F(1) &= \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', i')} b_j(1) \right) - \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', n+1')} b_j(1) \right) \\
&\quad - a_1 \sum_{j \in L_1} b_j(1) - b_1(1) S_1 \\
&= \sum_{i \notin L_1} \left(\sum_{j \in L(i', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) \\
&\quad - a_1 \sum_{j \in L_1} b_j(1) - b_1(1) S_1 \\
&= \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) \\
&\quad - (1-c) a_1 S_1 - (S_a - c a_1 - c S_1) S_1
\end{aligned}$$

Putting in equation (5.21) we get

$$\begin{aligned}
&(1-c)(n-c+1) - (n-2c+2-S_a)(S_a - c a_1 - c S_1) + (n-c+2) a_1 S_a \\
&- (1+c) a_1 (S_a - c a_1 - c S_1) - (n+1) a_1^2 - (n+1) c a_1 S_1 - c(1-c) a_1 S_1 \\
&+ c \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) - c(S_a - c a_1 - c S_1) S_1 = 0
\end{aligned}$$

$$\begin{aligned}
& \text{or } (1-c)(n-c+1) - (n-2c+2)S_a + S_a^2 + c(n-2c+2-2S_a)S_1 \\
& + (c(n-2c+2) + (n-3c+1)S_a)a_1 + (c+c^2-n-1)a_1^2 + c^2S_1^2 \\
& + c(3c-n-1)a_1S_1 + c\sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) = 0
\end{aligned}
\tag{5.22}$$

Lemma 5.3.19: Let i and j be fixed, $1 \leq i < j \leq n+1$, and let $l \in \Omega$, $l \notin L(i, j)$. Then

$$\begin{aligned}
& UL(i', k') = UL(j', k') \\
& k \in L(j', l') \quad k \in L(i', l')
\end{aligned}$$

Proof: Both sides are equal to

$$\Omega \setminus L(i, l) UL(j, l) UL(i, j)$$

We use lemma 5.3.19 to simplify the last term in equation (5.22):

$$\begin{aligned}
& \sum_{j \in L(i', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \\
& = \sum_{j \in L(i', i')} a_j + c \sum_{j \in L(i', i')} \left(\sum_{k \in L(i', j')} a_k \right) - c \sum_{j \in L(i', i')} \left(\sum_{k \in L_1} a_k \right) \\
& - \sum_{j \in L(i', n+1')} a_j - c \sum_{j \in L(i', n+1')} \left(\sum_{k \in L(i', j')} a_k \right) + c \sum_{j \in L(i', n+1')} \left(\sum_{k \in L_1} a_k \right) \\
& = (q-1)ca_1 + ((q-2)c+1) \sum_{j \in L(i', i')} a_j - (q-1)c \sum_{k \in L_1} a_k \\
& - \sum_{j \in L(i', n+1')} a_j - c \sum_{j \in L(i', n+1')} \left(\sum_{k \in L(i', j')} a_k \right) + (q-1)c \sum_{k \in L_1} a_k
\end{aligned}$$

By lemma 5.3.19,

$$\sum_{j \in L(i', n+1')} \left(\sum_{k \in L(i', j')} a_k \right) = \sum_{j \in L(i', n+1')} \left(\sum_{k \in L(i', j')} a_k \right)$$

$$\begin{aligned}
& \text{Hence } \sum_{j \in L(i', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \\
&= (n-c)a_i + (n-2c+1) \sum_{j \in L(i', i')} a_j - \sum_{j \in L(i', n+1')} a_j \\
&\quad - c \sum_{j \in L_1''} \left(\sum_{k \in L(i', j')} a_k \right)
\end{aligned}$$

$$\begin{aligned}
& \text{Therefore } \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) \\
&= (n-c) \sum_{i \notin L_1} a_i^2 + (n-2c+1) \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', i')} a_j \right) - \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', n+1')} a_j \right) \\
&\quad - c \sum_{i \notin L_1} a_i \left(\sum_{j \in L_1''} \left(\sum_{k \in L(i', j')} a_k \right) \right) \\
&= (n-c) \left(T - \sum_{i \in L_1'} a_i^2 \right) + 2(n-2c+1) \sum_{\substack{L \ni 1 \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{1\} \\ k < l}} a_k a_l \right) \\
&\quad - 2 \sum_{\substack{L \ni n+1 \\ L \not\ni 1}} \left(\sum_{\substack{k, l \in L \setminus \{n+1\} \\ k < l}} a_k a_l \right) - 2c \sum_{i \in L_1''} \sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k < l}} a_k a_l \right) \\
&= (n-c) \left(T - \sum_{i \in L_1'} a_i^2 \right) + 2(n-2c+1) \sum_{\substack{L \ni 1 \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{1\} \\ k < l}} a_k a_l \right) \\
&\quad - 2(P_{n+1} - \sum_{\substack{k, l \in L_1 \\ k < l}} a_k a_l) - 2c \sum_{i \in L_1''} \sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k < l}} a_k a_l \right)
\end{aligned}$$

$$\begin{aligned} & \text{Hence } c \sum_{i \notin L_1} a_i \left(\sum_{j \in L(1', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) \cdot \\ & = c(n-c)T - c(n-c) \sum_{i \in L_1} a_i^2 + 2c(n-2c+1) \sum_{\substack{L \ni 1 \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{1\} \\ k < l}} a_k a_l \right) \end{aligned}$$

$$- 2cP_{n+1} + 2c \sum_{\substack{k, l \in L_1 \\ k < l}} a_k a_l - 2c^2 \sum_{i \in L_1} \left(\sum_{\substack{L \ni i \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{i\} \\ k < l}} a_k a_l \right) \right)$$

Using equation (5.19) we get

$$\begin{aligned} & c \sum_{i \notin L_1} a_i \left(\sum_{j \in L(1', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) \\ & = c(n-c)T - c(n-c)a_1^2 - c(n-c) \sum_{i \in L_1} a_i^2 - 2cP_{n+1} + 2ca_1S_1 \\ & + (n-2c+1)((1+c)a_1^2 + (1-c-2S_a)a_1 + 2cP_{n+1} - 2c \sum_{\substack{k, l \in L_1 \\ k < l}} a_k a_l) + 2c \sum_{\substack{k, l \in L_1 \\ k < l}} a_k a_l \\ & - c \sum_{i \in L_1} ((1+c)a_i^2 + (1-c-2S_a)a_i + 2cP_{n+1} - 2c \sum_{\substack{k, l \in L(i', n+1') \\ k < l}} a_k a_l) \\ & = c(n-c)T - c(n-c)a_1^2 - c(n-c) \sum_{i \in L_1} a_i^2 + (n-2c+1)(1-c-2S_a)a_1 \\ & + 2c(n-2c+1)P_{n+1} - 2c(n-2c+1)P_{n+1} - 2c(n-2c+1) \sum_{k, l \in L_1, k < l} a_k a_l \\ & - 2cP_{n+1} + 2ca_1S_1 + 2c \sum_{k, l \in L_1, k < l} a_k a_l - c(1+c) \sum_{i \in L_1} a_i^2 - c(1-c-2S_a)S_1 \\ & + 2c^2(q-1)P_{n+1} + 2c^2 \sum_{i \in L_1} \left(\sum_{\substack{k, l \in L(i', n+1') \\ k < l}} a_k a_l \right) \end{aligned}$$

$$\begin{aligned}
&= c(n-c)T - c(n-c)a_1^2 - c(n-c)\sum_{i \in L_1} a_i^2 + (n-2c+1)(1+c)a_1^2 \\
&+ (n-2c+1)(1-c-2S_a)a_1 + 2c(n-2c+1)P_{n+1} - 2c(n-2c+1)\sum_{\substack{k, l \in L_1 \\ k < l}} a_k a_l \\
&- 2cP_{n+1} + 2ca_1S_1 + 2c\sum_{\substack{k, l \in L_1 \\ k < l}} a_k a_l - c(1+c)\sum_{i \in L_1} a_i^2 - c(1-c-2S_a)S_1 \\
&- 2c^2(q-1)P_{n+1} + 2c^2((q-2)a_1S_1 + (q-3)\sum_{\substack{k, l \in L_1 \\ k < l}} a_k a_l) \\
&= c(n-c)T + (n-c^2-c+1)a_1^2 - c(n+1)\sum_{i \in L_1} a_i^2 + (n-2c+1)(1-c-2S_a)a_1 \\
&- 2c^2P_{n+1} + 2c(n+1-2c)a_1S_1 - c(1-c-2S_a)S_1 - 2c^2\sum_{\substack{k, l \in L_1 \\ k < l}} a_k a_l
\end{aligned}$$

Putting in equation (5.22), we get

$$\begin{aligned}
&(1-c)(n-c+1) - (n-2c+2)S_a + S_a^2 + (c(n-2c+2)+(n-3c+1)S_a)a_1 \\
&+ c(n-2c+2-2S_a)S_1 + (c+c^2-n-1)a_1^2 + c(3c-n-1)a_1S_1 + c^2S_1^2 \\
&+ c(n-c)T + (n-c^2-c-1)a_1^2 - c(n+1)\sum_{i \in L_1} a_i^2 + 2c(n+1-2c)a_1S_1 \\
&+ (n-2c+1)(1-c-2S_a)a_1 - 2c^2P_{n+1} - c(1-c-2S_a)S_1 \\
&- 2c^2\sum_{\substack{k, l \in L_1}} a_k a_l = 0
\end{aligned}$$

$$\begin{aligned}
& \text{or } (1-c)(n-c+1) - (n-2c+2)S_a + S_a^2 + c(n-c)T - 2c^2P_{n+1} \\
& + (n-c+1)(1-S_a)a_1 + c(n-c+1)S_1 + c(n-c+1)a_1S_1 + c^2S_1^2 \\
& - c(n+1)\sum_{i \in L_1} a_i^2 - 2c^2\sum_{\substack{k, l \in L_1 \\ k < l}} a_k a_l = 0
\end{aligned}$$

$$\begin{aligned}
& \text{or } (1-c)(n-c+1) - (n-2c+2)S_a + S_a^2 + c(n-c)T - 2c^2P_{n+1} \\
& + (n-c+1)(1-S_a)a_1 + c(n-c+1)S_1 + c(n-c+1)a_1S_1 \\
& - c(n-c+1)\sum_{i \in L_1} a_i^2 = 0
\end{aligned}$$

$$\begin{aligned}
& \text{or } (1-c)(n-c+1) - (n-2c+2)S_a + S_a^2 + c(n-c)T - 2c^2P_{n+1} \\
& + (n-c+1)(1-S_a)a_1 + c(n-c+1)\sum_{j=2}^q a_j + c(n-c+1)a_1\sum_{j=2}^q a_j \\
& - c(n-c+1)\sum_{j=2}^q a_j^2 = 0
\end{aligned}$$

There was nothing special about choosing $1 \in L_1$ for this calculation, we could have started with any i , $1 \leq i \leq q$, to get

$$\begin{aligned}
& (1-c)(n-c+1) - (n-2c+2)S_a + S_a^2 + c(n-c)T + (n-c+1)(1-S_a)a_i \\
& - 2c^2P_{n+1} + c(n-c+1)\sum_{\substack{j=1 \\ j \neq i}}^q a_j + c(n-c+1)a_i\sum_{\substack{j=1 \\ j \neq i}}^q a_j - c(n-c+1)\sum_{\substack{j=1 \\ j \neq i}}^q a_j^2 = 0
\end{aligned}$$

— (5.23)

Now let $j \in L_1$, $j \neq 1$. In particular, choose $j=2$.

From equation (5.9), $d_2(1) = (n-2c+2)b_2(1)$,

$$\text{or} \quad d_2(1) - (n-2c+2)b_2(1) = 0 \quad (5.24)$$

From equation (5.6), $b_2(1) = (1-c)a_2$, and from equation

$$(5.7), \quad d_2(1) = -(1+c)a_2b_2(1) + a_2S_b(1) + b_2(1)S_a + c(E_2(1)-F(1))$$

Putting in equation (5.24), we get

$$\begin{aligned} -(1+c)a_2b_2(1) + a_2S_b(1) + b_2(1)S_a + c(E_2(1)-F(1)) \\ - (n-2c+2)b_2(1) = 0 \end{aligned}$$

$$\begin{aligned} \text{or} \quad -(1+c)a_2b_2(1) + a_2S_b(1) + (S_a - n + 2c - 2)b_2(1) \\ + c(E_2(1)-F(1)) = 0 \end{aligned}$$

$$\begin{aligned} \text{or} \quad -(1+c)a_2(1-c)a_2 + a_2S_b(1) + (S_a - n + 2c - 2)(1-c)a_2 \\ + c(E_2(1)-F(1)) = 0 \end{aligned}$$

$$\begin{aligned} \text{or} \quad -(1-c^2)a_2^2 + a_2((n-c+2)S_a - (n+1)a_1 - (n+1)cS_1) \\ + (S_a - n + 2c - 2)(1-c)a_2 + c(E_2(1)-F(1)) = 0 \end{aligned}$$

$$\begin{aligned} \text{or} \quad (c^2 - 1 - (n+1)c)a_2^2 - (n+1)a_1a_2 + (n-2c+3)a_2S_a \\ - (n-2c+2)(1-c)a_2 - (n+1)ca_2 \sum_{j \in L_1} \frac{a_j}{2} + c(E_2(1)-F(1)) = 0 \end{aligned}$$

———— (5.25)

$$\begin{aligned}
E_2(1) &= \sum_{\substack{L \ni 2 \\ L \neq n+1}} \left(\sum_{\substack{k, l \in L \setminus \{2\} \\ k \neq l}} a_k b_l(1) \right) + \sum_{\substack{k, l \in L_1 \setminus \{2\} \\ k \neq l}} a_k b_l(1) \\
&= \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} b_j(1) \right) + \sum_{i \in L_1 \setminus \{2\}} a_i \left(\sum_{j \in L_1 \setminus \{i, 2\}} b_j(1) \right) \\
F(1) &= \sum_{\substack{L \ni n+1 \\ k \neq l}} \left(\sum_{k, l \in L \setminus \{n+1\}} a_k b_l(1) \right) = \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', n+1')} b_j(1) \right) \\
&= \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', n+1')} b_j(1) \right) + a_2 \sum_{j \in L_1 \setminus \{2\}} b_j(1) + b_2(1) \sum_{j \in L_1 \setminus \{2\}} a_j \\
&\quad + \sum_{i \in L_1 \setminus \{2\}} a_i \left(\sum_{j \in L_1 \setminus \{i, 2\}} b_j(1) \right)
\end{aligned}$$

$$\begin{aligned}
\text{Therefore } E_2(1) - F(1) &= \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} b_j(1) \right) \\
&\quad - \sum_{i \notin L_1} a_i \left(\sum_{j \in L(i', n+1')} b_j(1) \right) - a_2 \sum_{j \in L_1 \setminus \{2\}} b_j(1) - b_2(1) \sum_{j \in L_1 \setminus \{2\}} a_j \\
&= \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) - a_2 b_1(1) - a_2 \sum_{j \in L_1 \setminus \{2\}} b_j(1) \\
&\quad - a_1 b_2(1) - b_2(1) \sum_{j \in L_1 \setminus \{2\}} a_j \\
&= \sum_{i \notin L_1} \left(\sum_{j \in L(2', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) - a_2 (S_a - c a_1 - c \sum_{i \in L_1} a_i) \\
&\quad - (1-c) a_2 \sum_{j \in L_1 \setminus \{2\}} a_j - (1-c) a_1 a_2 - (1-c) a_2 \sum_{j \in L_1} a_j
\end{aligned}$$

$$\begin{aligned}
&= \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) - a_2 S_a + ca_1 a_2 + ca_2^2 \\
&+ ca_2 \sum_{i \in L_1 \setminus \{2\}} a_i - (1-c)a_2 \sum_{j \in L_1 \setminus \{2\}} a_j - (1-c)a_1 a_2 - (1-c)a_2 \sum_{i \in L_1 \setminus \{2\}} a_i \\
&= \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) - a_2 S_a + (2c-1)a_1 a_2 \\
&\quad + ca_2^2 + (3c-2)a_2 \sum_{j \in L_1 \setminus \{2\}} a_j
\end{aligned}$$

Putting in equation (5.25), we get

$$\begin{aligned}
&(c^2 - 1 - (n+1)c)a_2^2 - (n+1)a_1 a_2 + (n-2c+3)a_2 S_a - ca_2 S_a \\
&- (n-2c+2)(1-c)a_2 - (n+1)ca_2 \sum_{j \in L_1 \setminus \{2\}} a_j + c(2c-1)a_1 a_2 + c^2 a_2^2 \\
&+ c(3c-2)a_2 \sum_{j \in L_1 \setminus \{2\}} a_j + c \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) = 0 \\
&\text{or } (2c^2 - 1 - (n+1)c)a_2^2 + (2c^2 - c - n - 1)a_1 a_2 + (n-3c+3)a_2 S_a \\
&- (n-2c+2)(1-c)a_2 - c(n-3c+3)a_2 \sum_{j \in L_1 \setminus \{2\}} a_j + c \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} b_j(1) \right. \\
&\quad \left. - \sum_{j \in L(i', n+1')} b_j(1) \right) = 0 \tag{5.26}
\end{aligned}$$

It follows from lemma 5.3.19 and an easy rearrangement of terms that

$$\sum_{j \in L(2', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) = (1-c) \left(\sum_{j \in L(2', i')} a_j - \sum_{j \in L(i', n+1')} a_j \right)$$

$$\begin{aligned}
& \text{Therefore } c \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) \\
&= c(1-c) \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} a_j - \sum_{j \in L(i', n+1')} a_j \right) \\
&= 2c(1-c) \left(\sum_{\substack{L \ni 2 \\ L \not\ni n+1}} \left(\sum_{\substack{k, l \in L \setminus \{2\} \\ k < l}} a_k a_l \right) - (P_{n+1} - \sum_{\substack{k, l \in L(2', n+1') \\ k < l}} a_k a_l) \right)
\end{aligned}$$

Using equation (5.19), we get

$$\begin{aligned}
& c \sum_{i \notin L_1} a_i \left(\sum_{j \in L(2', i')} b_j(1) - \sum_{j \in L(i', n+1')} b_j(1) \right) \\
&= (1-c) \left((1+c)a_2^2 + (1-c-2S_a)a_2 + 2cP_{n+1} - 2c \sum_{\substack{k, l \in L(2', n+1') \\ k < l}} a_k a_l \right) \\
&\quad - 2c(1-c)P_{n+1} + 2c(1-c) \sum_{\substack{k, l \in L(2', n+1') \\ k < l}} a_k a_l \\
&= (1-c^2)a_2^2 + (1-c)(1-c-2S_a)a_2 + 2c(1-c)P_{n+1} - 2c(1-c)P_{n+1} \\
&\quad - 2c(1-c) \sum_{\substack{k, l \in L(2', n+1') \\ k < l}} a_k a_l + 2c(1-c) \sum_{\substack{k, l \in L(2', n+1') \\ k < l}} a_k a_l \\
&\quad + 2c(1-c)a_2 \sum_{j \in L(2', n+1')} a_j \\
&= (1-c^2)a_2^2 + (1-c)(1-c-2S_a)a_2 + 2c(1-c)a_2 \sum_{j \in L_1 \setminus \{2\}} a_j \\
&= (1-c^2)a_2^2 + (1-c)(1-c-2S_a)a_2 + 2c(1-c)a_1 a_2 \\
&\quad + 2c(1-c)a_2 \sum_{j \in L_1 \setminus \{2\}} a_j
\end{aligned}$$

Putting in equation (5.26), we get

$$\begin{aligned}
 & (2c^2 - 1 - (n+1)c)a_2^2 + (2c^2 - c - n - 1)a_1a_2 + (n-3c+3)a_2S_a \\
 & - (n-2c+2)(1-c)a_2 - c(n-3c+3)a_2 \sum_{j \in L_1'' \setminus \{2\}} a_j + (1-c^2)a_2^2 \\
 & + (1-c)(1-c-2S_a)a_2 + 2c(1-c)a_1a_2 + 2c(1-c)a_2 \sum_{j \in L_1'' \setminus \{2\}} a_j = 0 \\
 \text{or } & -c(n-c+1)a_2^2 - (n-c+1)a_1a_2 + (n-c+1)a_2S_a \\
 & + (c-1)(n-c+1)a_2 - c(n-c+1)a_2 \sum_{j \in L_1'' \setminus \{2\}} a_j = 0
 \end{aligned}$$

Since $n-c+1 = n+a \neq 0$ in K , we get

$$\begin{aligned}
 & -ca_2^2 - a_1a_2 + a_2S_a + (c-1)a_2 - ca_2 \sum_{j \in L_1'' \setminus \{2\}} a_j = 0 \\
 \text{or } & -ca_2^2 - a_1a_2 + a_2S_a + (c-1)a_2 - ca_2 \sum_{j=3}^q a_j = 0
 \end{aligned}$$

As in the earlier case, there was nothing special about choosing 1 and 2 for the derivation of this relation, we could have started with any $i, j, 1 \leq i, j \leq q, i \neq j$. That gives us $q(q-1)$ equations

$$ca_i^2 + a_ia_j - a_iS_a + (1-c)a_i + ca_i \sum_{\substack{k=1 \\ k \neq i, k \neq j}}^q a_k = 0 \quad (5.27)$$

We now consider the two cases in (5.18), viz.,

$$(i) \quad S_a = 1, T = 1, P_{n+1} = 0.$$

$$(ii) \quad S_a = -n, T = n, P_{n+1} = \frac{n(n-c)}{2c}$$

$$\text{Case (i): } S_a = 1, T = 1, P_{n+1} = 0.$$

From equation (5.23), we get

$$\begin{aligned} (1-c)(n-c+1) - (n-2c+2) + 1 + c(n-c) + c(n-c+1) \sum_{\substack{j=1 \\ j \neq i}}^q a_j \\ + c(n-c+1) a_i \sum_{\substack{j=1 \\ j \neq i}}^q a_j - c(n-c+1) \sum_{\substack{j=1 \\ j \neq i}}^q a_j^2 = 0 \end{aligned}$$

$$\text{or} \quad c(n-c+1) \sum_{\substack{j=1 \\ j \neq i}}^q a_j + c(n-c+1) a_i \sum_{\substack{j=1 \\ j \neq i}}^q a_j - c(n-c+1) \sum_{\substack{j=1 \\ j \neq i}}^q a_j^2 = 0$$

Since $c \neq 0$, $n-c+1 = n+a \neq 0$ in K , we get that for $1 \leq i \leq q$,

$$\sum_{\substack{j=1 \\ j \neq i}}^q a_j + a_i \sum_{\substack{j=1 \\ j \neq i}}^q a_j - \sum_{\substack{j=1 \\ j \neq i}}^q a_j^2 = 0 \quad (5.28)$$

From equation (5.27), we get

$$ca_i^2 + a_i a_j - a_i - (c-1)a_i + ca_i \sum_{\substack{k=1 \\ k \neq i, k \neq j}}^q a_k = 0$$

or, for $1 \leq i, j \leq q$, $i \neq j$,

$$ca_i^2 + a_i a_j - ca_i + ca_i \sum_{\substack{k=1 \\ k \neq i, k \neq j}}^q a_k = 0 \quad (5.29)$$

Suppose $a_1 = a_2 = \dots = a_q = \gamma$. From equation (5.28),

$$(q-1)\gamma + (q-1)\gamma^2 - (q-1)\gamma^2 = 0$$

or $(q-1)\gamma = 0$

But $\text{ch}(K) > |a| = c-1 = \frac{n}{q}-1 = q(q^{m-2} + q^{m-3} + \dots + 1)$. Since $m \geq 3$, $\text{ch}(K) > q$, so $q-1 \neq 0$ in K . Hence $\gamma = 0$. Therefore if all a_j 's on a line containing $n+1$ are equal, then all of them are zero.

Now suppose $a_i \neq a_j$ for $i \neq j$, $i, j \in L_1'$. In particular, say $a_1 \neq a_2$.

$$\text{Let } S_2 = \sum_{j=3}^q a_j, \quad T_2 = \sum_{j=3}^q a_j^2.$$

Putting $i=1$, $j=2$ in equation (5.28), we get

$$a_2 + S_2 + a_1 a_2 + a_1 S_2 - a_2^2 - T_2 = 0 \quad (5.30)$$

$$a_1 + S_2 + a_1 a_2 + a_2 S_2 - a_1^2 - T_2 = 0 \quad (5.31)$$

Subtracting equation (5.30) from equation (5.31), we get

$$(a_1 - a_2) - (a_1 - a_2)S_2 - (a_1^2 - a_2^2) = 0$$

Since $a_1 \neq a_2$, $1 - S_2 - (a_1 + a_2) = 0$,

or $S_2 = 1 - (a_1 + a_2) \quad (5.32)$

Putting $i=1$, $j=2$ in equation (5.29), we get

$$ca_1^2 + a_1a_2 - ca_1 + ca_1S_2 = 0 \quad (5.33)$$

Therefore from equation (5.32),

$$ca_1^2 + a_1a_2 - ca_1 + ca_1(1-(a_1+a_2)) = 0$$

or
$$(1-c)a_1a_2 = 0$$

Since $c \neq 1$, $a_1a_2 = 0$, that is, $a_1=0$ or $a_2=0$. Without loss of generality, let $a_2=0$. Since $a_1 \neq a_2$, $a_1 \neq 0$.

Subcase (i'): $q=2$

If $q=2$, $S_2=0$, $T_2=0$. Hence from equation (5.32), we get that $a_1=1$.

Subcase (i''): $q \geq 3$

Let $S_3 = \sum_{j=4}^q a_j$. From equation (5.33), we get

$$ca_1^2 + a_1a_2 - ca_1 + ca_1a_3 + ca_1S_3 = 0 \quad (5.34)$$

Also, from equation (5.29), with $i=1$, $j=3$, we get

$$ca_1^2 + a_1a_3 - ca_1 + ca_1a_2 + ca_1S_3 = 0 \quad (5.35)$$

Subtracting equation (5.35) from equation (5.34), we get

$$a_1(a_2-a_3) - ca_1(a_2-a_3) = 0$$

or
$$(1-c)a_1(a_2-a_3) = 0$$

Since $a_1 \neq 0$ and $c \neq 1$ in K ,

$$a_2 = a_3 = 0$$

Similarly $a_4=a_5= \dots =a_q=0$. Therefore $S_2=0$. Hence

from equation (5.32), $a_1 = 1$.

There was nothing special about 1 and 2, what we have shown here is that either all a_j 's on a line containing $n+1$ are zero, or one of them is 1 and all others are zero. Since there are exactly c lines containing $n+1$, and their union is Ω , we get that all a_i are 0 or 1, and the number of ones is less than or equal to c . Since $S_a = \sum_i a_i = 1$, and $\text{ch}(K) > |a| = c-1$, this is possible only if $a_i = 1$ for exactly one i , and $a_j = 0$ if $j \neq i$.

Therefore $\sigma(x_1) = x_i$ for some i , $1 \leq i \leq n$.

Case (ii): $S_a = -n$, $T = n$, $P_{n+1} = \frac{n(n-c)}{2c}$.

From equation (5.23), we get

$$\begin{aligned} & (1-c)(n-c+1) - (n-2c+2)(-n) + n^2 + c(n-c)n - 2c^2 \frac{n(n-c)}{2c} \\ & + (n-c+1)(1+n)a_i + c(n-c+1) \sum_{\substack{j=1 \\ j \neq i}}^q a_j + c(n-c+1) a_i \sum_{\substack{j=1 \\ j \neq i}}^q a_j \\ & - c(n-c+1) \sum_{\substack{j=1 \\ j \neq i}}^q a_j^2 = 0 \end{aligned}$$

$$\begin{aligned} \text{or } & 2n^2 + 3n - 3nc + c^2 - 2c + 1 + (n+1)(n-c+1)a_i \\ & + c(n-c+1) \sum_{\substack{j=1 \\ j \neq i}}^q a_j + c(n-c+1) a_i \sum_{\substack{j=1 \\ j \neq i}}^q a_j - c(n-c+1) \sum_{\substack{j=1 \\ j \neq i}}^q a_j^2 = 0 \end{aligned}$$

Since $2n^2+3n-3nc+c^2-2c+1 = (2n+1-c)(n-c+1)$ and $n-c+1 \neq 0$ in K , we get that for $1 \leq i \leq q$,

$$(2n+1-c) + (n+1)a_i + c \sum_{\substack{j=1 \\ j \neq i}}^q a_j + ca_i \sum_{\substack{j=1 \\ j \neq i}}^q a_j - c \sum_{\substack{j=1 \\ j \neq i}}^q a_j^2 = 0 \quad (5.36)$$

From equation (5.27), we get

$$ca_i^2 + a_i a_j + na_i - (c-1)a_i + ca_i \sum_{\substack{k=1 \\ k \neq i, k \neq j}}^q a_k = 0$$

Therefore for $1 \leq i, j \leq q$, $i \neq j$,

$$ca_i^2 + a_i a_j + (n-c+1)a_i + ca_i \sum_{\substack{k=1 \\ k \neq i, k \neq j}}^q a_k = 0 \quad (5.37)$$

Suppose $a_1 = a_2 = \dots = a_q = \delta$. From equation (5.37),

$$c\delta^2 + \delta^2 + (n-c+1)\delta + c(q-2)\delta^2 = 0$$

$$\text{or} \quad (n-c+1)\delta(\delta+1) = 0$$

Since $n-c+1 = n+a \neq 0$ in K , $\delta = 0$, or $\delta = -1$. Hence if all a_j 's on a line containing $n+1$ are equal, then all of them are zero or all of them are -1 .

Now suppose $a_i \neq a_j$ for $i \neq j$, $i, j \in L_1$. In particular say $a_1 \neq a_2$.

$$\text{As before, let } S_2 = \sum_{j=3}^q a_j, \quad T_2 = \sum_{j=3}^q a_j^2.$$

Putting $i=1$, $i=2$ in equation (5.36), we get

$$(2n+1-c)+(n+1)a_1+ca_2+cS_2+ca_1a_2+ca_1S_2-ca_2^2-cT_2=0 \quad (5.38)$$

$$(2n+1-c)+(n+1)a_2+ca_1+cS_2+ca_1a_2+ca_2S_2-ca_1^2-cT_2=0 \quad (5.39)$$

Subtracting equation (5.39) from equation (5.38), we get

$$(n+1)(a_1-a_2) - c(a_1-a_2) + cS_2(a_1-a_2) + c(a_1^2-a_2^2) = 0$$

$$\text{Since } a_1 \neq a_2, (n+1-c) + cS_2 - c(a_1+a_2) = 0.$$

$$\text{or } cS_2 = -(n-c+1) - c(a_1+a_2) = 0 \quad (5.40)$$

Putting $i=1$, $j=2$ in equation (5.37), we get

$$ca_1^2 + a_1a_2 + (n-c+1)a_1 + ca_1S_2 = 0$$

$$\text{or } ca_1^2 + a_1a_2 + (n-c+1)a_1 + a_1(-(n-c+1)-c(a_1+a_2)) = 0$$

$$\text{or } (1-c)a_1a_2 = 0$$

Since $c \neq 1$, $a_1a_2 = 0$, that is, $a_1 = 0$ or $a_2 = 0$. Without loss of generality, let $a_2 = 0$. Since $a_1 \neq a_2$, $a_1 \neq 0$.

Subcase (ii'): $q=2$

If $q=2$, $S_2 = 0$, $T_2 = 0$. Hence we get $ca_1 = -(n-c+1)$, or

$$a_1 = \frac{-(n-c+1)}{c}. \text{ Putting in equation (5.39), we get}$$

$$2n+1-c-(n-c+1)-\frac{(n-c+1)^2}{c} = 0, \text{ or } nc = (n-c+1)^2.$$

Subcase (ii''): $q \geq 3$

Putting $i=1$, $j=3$ in equation (5.37), we get

$$ca_1^2 + a_1a_3 + (n-c+1)a_1 + ca_1(S_2-a_3) = 0$$

$$\text{Since } a_1 \neq 0, ca_1 + a_3 + (n-c+1) + cS_2 - ca_3 = 0$$

$$\text{or } ca_1 + a_3 + (n-c+1) - (n-c+1) - ca_1 - ca_3 = 0$$

$$\text{or } (1-c)a_3 = 0. \text{ Since } c \neq 1, a_3 = 0.$$

Similarly, $a_4 = a_5 = \dots = a_q = 0$. So $S_2 = 0$, $T_2 = 0$ and as in subcase (ii'), we get $nc = (n-c+1)^2$.

Claim: In K , $nc \neq (n-c+1)^2$.

$$\text{Proof: } n+1-c = (q^m-1)/(q-1) - n/q$$

$$\begin{aligned} &= \frac{q^m-1}{q-1} - \frac{1}{q} \frac{q^m-q}{q-1} = \frac{q^m-1}{q-1} - \frac{q^{m-1}-1}{q-1} \\ &= \frac{q^m-q^{m-1}}{q-1} = q^{m-1} \end{aligned}$$

$$\text{Therefore } (n-c+1)^2 = q^{2m-2} \equiv 0 \pmod{q^2}$$

On the other hand

$$\begin{aligned} nc &= \frac{n^2}{q} = \frac{1}{q} \frac{(q^m-q)^2}{(q-1)^2} = \frac{q(q^{m-1}-1)^2}{(q-1)^2} \\ &= q(q^{m-2}+q^{m-3}+\dots+1)^2 \end{aligned}$$

$$\text{Since } m \geq 3, \quad nc \equiv q \pmod{q^2}$$

But we have seen earlier that $q \neq 0$ in K . Hence the claim.

Therefore $a_i \neq a_j$ for $i \neq j$, $i, j \in L_1'$ gives a contradiction. Hence all a_i 's on any line containing $n+1$ are equal, and their value is 0 or -1. Let s be the number of lines containing $n+1$ on which all a_i 's are -1. Then

$S_a = -sq$. But in this case, $S_a = -n = -cq$. Since $q \neq 0$ in K , $s-c = 0$ in K . But $\text{ch}(K) \geq c$ and $s \leq c$ as an integer, so $s = c$ in K , and hence $s = c$ as an integer.

Therefore $a_i = -1$ on all lines containing $n+1$. Since the union of all lines passing through $n+1$ is Ω , we get that $a_i = -1 \forall i, 1 \leq i \leq n$.

Therefore $\sigma(x_1) = x_{n+1}$

Putting together cases (i) and (ii), we see that $\sigma(x_1) \in \{x_1, x_2, \dots, x_{n+1}\}$. But this shows that $\text{Aut}(A)$ permutes $\{x_1, x_2, \dots, x_{n+1}\}$ and hence $\text{Aut}(A) \subseteq \Sigma_{n+1}$.

By corollary 3.3.4, $\text{Aut}(A) \cong \text{PFL}(m, q)$.

LIST OF REFERENCES

1. H.P. ALLEN: Non-Associative Algebras Associated with Doubly Transitive Permutation Groups: S_{n+1} , Journal of Algebra, Vol. 91 (1984), 265-279.
2. H.P. ALLEN: On Automorphism Groups of Non-Associative Algebras Associated with Doubly Transitive Groups, Journal of Algebra, Vol. 91 (1984), 258-264.
3. E. ARTIN: Geometric Algebra, Interscience Publishers Inc., New York.
4. P.J. CAMERON, J.M. GOETHALS and J.J. SIEDEL: The Krein condition, spherical designs, Norton algebras and permutation groups, Indagationes Mathematicae, Vol. 40 (1978), 196-206.
5. Y. EGAWA and H. SUZUKI: Automorphism groups of multilinear mappings, Journal of Mathematical Society of Japan, Vol. 37 (1985), 135-155.
6. Y. EGAWA and H. SUZUKI: Automorphism groups of Σ_{n+1} -invariant trilinear forms, Hokkaido Mathematical Journal, Vol. 14 (1985), 39-42.
7. D. FROHARDT: A Trilinear Form for the Third Janko Group, Journal of Algebra, Vol. 83 (1983), 349-379.
8. R. GRIESS: The Friendly Giant, Inventiones Mathematicae, Vol. 69 (1982), 1-102.
9. K. HARADA: On a commutative nonassociative algebra associated with a multiply transitive group, Journal of the Faculty of Science, The University of Tokyo, Vol. 28 (1982), 843-849.
10. K. HARADA: On a Commutative Non-Associative Algebra Associated with a Doubly Transitive Group, Journal of Algebra, Vol. 91 (1984), 192-206.

11. K. HARADA: On commutative nonassociative algebras associated with the doubly transitive permutation groups $\text{PSL}_m(q)$, $m \geq 3$, Communications in Algebra, Vol. 12 (1984), 2291-2313.
12. B. HUPPERT: Endlichen Gruppen, I, Springer-Verlag Berlin-Heidelberg-New York, 1967.
13. C. JORDAN: Mémoire sur l'équivalence des formes, J. Éc. Pol. XLVIII (1880), 112-150.
14. M. KITAZOME: Unpublished note.
15. H. MATSUMURA and P. MONSKY: On the automorphisms of hypersurfaces, Journal of Mathematics of Kyoto University, Vol. 3 (1964), 347-361.
16. C.H. SAH: Alternating and Symmetric Multilinear Forms and Poincaré Algebras, Communications in Algebra, Vol. 2 (1974), 91-116.
17. J.E. SCHNEIDER: Orthogonal Groups of Nonsingular Forms of Higher Degree, Journal of Algebra, Vol. 27 (1973), 112-116.
18. S.D. SMITH: Nonassociative Commutative Algebras for Triple Covers of 3-Transposition Groups, Michigan Math. Journal, Vol. 24 (1977), 273-287.
19. H. SUZUKI: Automorphism Groups of Multilinear Maps, Osaka Journal of Mathematics, Vol. 20 (1983), 659-673.
20. H. SUZUKI: Commutative Algebras Associated with a Doubly Transitive Group, preprint.
21. J. TITS: Résumé de Cours, Annuaire du Collège de France, 1982-1983, 89-102.
22. J. TITS: Remarks on Griess' construction of the Griess-Fischer sporadic group, I, II, III, IV, Mimeographed letters, December 1982-July 1983.
23. J. TITS: Le Monstre (d'après R. Griess, B. Fischer et al.), Séminaire Bourbaki, exposé n°620, novembre 1983, à paraître dans Astérisque.

24. J. TITS: On R. Griess' "Friendly giant", Inventiones Mathematicae, Vol. 78 (1984), 491-499.
25. M. WAJIMA: Non-Associative Algebras and Their Automorphism Groups, Ph.D. Thesis, The Ohio State University, 1984.